Computer Forensik

Lerneinheit 3: Fall 2: Ein kompromittierter Server

Prof. Dr. Christoph Karg

Studiengang Informatik
Hochschule Aalen

Wintersemester 2013/2014

Ausgangssituation

- Bei einem Linux Server wurden Unregelmäßigkeiten festgestellt
- Folgende Beweisstücke wurden sicher gestellt:
  - Speicherdump des Servers
  - Virtuelle Maschine des Servers
  - Netzwerkmitschnitt des Angriffs

Zu klärende Fragen

1. Welcher Dienst und welcher Account lösten einen Alarm aus?
2. Welches Betriebssystem läuft auf dem Server?
3. Wie lautet die IP des Angreifers und die IP des angegriffenen Systems?
4. Wie kann man die Partitionen der virtuellen Maschine unter Linux mounten?
5. Welche Prozesse laufen auf dem Server?
6. Welcher Service wurde angegriffen?
7. Welche Art von Angriff wurde durchgeführt?
8. Welche Schwachstelle wurde ausgenutzt?
9. Wie ist der Angriff abgelaufen?

Zu klärende Fragen (Forts.)

8. Welche Angriffe waren erfolgreich, welche nicht?
9. Welche Konsequenzen hatte der Angriff?
10. Hat der Angreifer Dateien auf den Server heruntergeladen? Falls ja, welche Dateien waren dies und was war der Inhalt der Dateien?
11. Welche Spuren hat der Angreifer auf dem Server hinterlassen?
12. Was kann man über den Angreifer aussagen? (Motivation, Qualifikation)
13. Handelt es sich um einen automatisierten Angriff?
14. Wie hätte der Angriff verhindert werden können?

Nützliche Werkzeuge

- Volatilitux $\rightsquigarrow$ Analyse von Speicherdumps eines Linuxsystems
- VBoxManage $\rightsquigarrow$ Werkzeug zur Arbeit mit virtuellen Maschinen
- Wireshark $\rightsquigarrow$ Analyse des Netzwerkverkehrs
- Mount $\rightsquigarrow$ Einbinden einer Laufwerkssicherung
- Google $\rightsquigarrow$ Recherche