michael.engel [☺] hs-coburg.de

Praktikum zur Vorlesung
Malware-Analyse und Reverse Engineering
Sommersemester 2017

Praktikumsaufgabe 9

Besprechung am Donnerstag, 22. Juni 2017

Hinweise: Praktikumsaufgaben müssen in der vorgegebenen Zeit in den eingeteilten Gruppen bearbeitet werden. Die Lösung der Aufgaben wird bewertet, jedes Gruppenmitglied soll Fragen zu den einzelnen Aufgaben beantworten können. Bei Unklarheiten und Rückfragen wird selbstverständlich eine Hilfestellung gegeben.

9.1 Rootkit

In dieser Praktikumsaufgabe soll ein einfaches rootkit entwickelt werden.

- Schreiben Sie ein Programm, das permanent eine "böswillige" Aktion ausführt, z.B. Rechenzeit verschwendet, indem es alle Ziffern von π berechnet und in eine Datei schreibt... (zur Not tut's natürlich auch eine einfache Endlosschleife, die pro Durchlauf ein Zeichen in eine Datei schreibt, möglichst mit Verzögerung zwischen den Durchläufen)

  Starten Sie das Programm im Hintergrund als Systemadministrator: `$ sudo nohup ./prog &`

- Finden Sie möglichst viele Methoden, mit denen Sie feststellen können, dass Ihr Programm gerade läuft (z.B. das ps-Kommando, Anzeigen der erzeugten Datei, ...). Dies sind die Methoden, die ein rootkit manipuliert, um sich vor "neugierigen" Blicken zu verbergen.

- Erweitern Sie nun Ihr Programm, so dass es ein einfaches (user mode) rootkit darstellt, also seine Existenz vor Benutzern so gut wie möglich verbirgt. Verwenden Sie dabei schon bekannte Methoden wie das Überladen von Library-Funktionen oder das tracing von Systemaufrufen.

  Hinweis: Damit Sie keine Systemdateien verändern müssen, gehen Sie davon aus, dass der Benutzer nur eine von Ihrem Programm (mit fork und execl) gestartete Shell benutzen kann.