5.1 Dynamic Analysis

(a) Erläutern Sie Unterschiede zwischen Software- und Hardware-Breakpoints.

(b) Alle Interrupt-Instruktionen sind 2-Byte groß (hexadezimal CD XX wobei XX ein Immediate ist). Allerdings ist die INT3-Instruktion nur ein Byte groß (hexadezimal CC). Warum?

(c) Wenn ein Software-Breakpoint erreicht wird, führt der Debugger die ursprüngliche Instruktion aus. Wie stellt der Debugger sicher, dass der Breakpoint (die INT3-Instruktion) bestehen bleibt und beim nächsten Mal wieder auslöst?

5.2 Sandbox Evasion

(a) Versetzen Sie sich in die Rolle eines Schadsoftware-Autors. Überlegen Sie sich Möglichkeiten, um zu erkennen oder zu vermeiden, dass ihre Schadsoftware in einer Sandbox ausgeführt wird.