Bachelorthesis-Aufgabe

Exploit Detektion mittels "Memory Tracing"

ID	IBTE1-2-13
Studierende	Ramon Spahr Jonas Wagner
Betreuer	Dr. Endre Bangerter Dominic Fischer
Experten	Dr. Federico Flueckiger
Aufgabe	Memory Tracing ist eine neuartige Technologie um unbekannte Software dynamisch zu analysieren. Dabei wird der Zustand eines Systems (RAM / CPU) überwacht und Zustandsänderungen für spätere Analysen gespeichert. Existierende Memory Tracing Implementationen erzeugen vielversprechende Resultate im Bereich der Malware Analyse. Ein Teil der Malware Analyse ist die Suche nach verwendeten Exploits um in ein System einzudringen oder um erhöhte Rechte in einem System zu erlangen. Ziel dieser Arbeit ist es, zu überprüfen inwiefern sich Memory Tracing eignet um Exploits zu entdecken und zu kategorisieren. Mögliche Ziele der Thesis sind: • Entdecken von Exploits mittels Memory Tracing • Kategorisierung der verschiedenen Exploitklassen (Stack Overflow, Heap Spray, ROP, Privilege Escalation Exploit, Local / Remote Code Execution, Kernel / User Mode, etc.) • Detektion und Analyse der obigen Exploitklassen mittels Memory Tracing • Entdecken der verschiedenen Phasen einer Infektion (Exploit, Payload,etc.) • Entwicklung von Tools um genannte Ziele zu erfüllen