Handout – Reverse Engineering

Viele Unterbereiche, unter anderem

* Anti-Viren-Development
* Cracking
* Game-Hacking

**2 Möglichkeiten** um ein laufendes Programm zu modifizieren

* **„External“**
  + Verändern und Überwachen von Programmspeicher des Zielprogramms durch ein Externes Programm, das die Windows-API benutzt.
* **„Internal“**
  + Zielprogramm wird dazu gezwungen eine Payload-DLL zu laden
  + Die DLL „ist“ dann quasi der Zielprozess.
  + Es ist auf diesem Weg möglich die Funktionen des Zielprogramms während der Ausführung aufzurufen.
  + Durch Pointer ist die Veränderung des Programmspeichers sehr einfach
  + „Hooking“1 wird damit möglich
  + Schwieriger als External, da mehr Sachen beachtet werden müssen, z.B. welche Architektur der Zielprozess hat, etc.
  + Ein „DLL-Injektor“2 wird für diese Methode benötigt

1Umleiten des Programmflusses auf eigene Funktionen  
2Ein Programm, das Programme dazu bringt, ungewollt DLLs zu laden