



SySS-Workshop: Exploit Development

Im Rahmen dieses zweitägigen *Exploit Development*-Workshops werden die theoretischen und praktischen Grundlagen für die Funktionsweise sowie die Entwicklung von *Exploits* vermittelt.

Inhalt:

- **Besonderheiten verschiedener Zielplattformen:**
 - Prozessorarchitekturen: x86, ARM, PowerPC, MIPS
 - Betriebssysteme: WINDOWS, UNIX/LINUX, MAC OS.
- **Verschiedene Formen der Schwachstellenanalyse:**
 - Statische Codeanalyse
 - Analyse zur Laufzeit
- **Tools of the Trade:**

Wichtige Werkzeuge für die Exploit-Entwicklung wie Debugger, Disassembler und *Exploit*-Frameworks

- **Ausnutzen verschiedener Schwachstellentypen:**
 - Fehler in der Hard- und Softwarearchitektur
 - Fehler in der Anwendungslogik
 - *Buffer Overflow*-Schwachstellen
 - *Format String*-Schwachstellen
- **Schutzmaßnahmen und Möglichkeiten, diese zu umgehen:**
 - Stack Cookies
 - SafeSEH
 - Data Execution Prevention (DEP)
 - Address Space Layout Randomization (ASLR).

Zielgruppe:	Administratoren, Softwareentwickler, Sicherheitsspezialisten, IT-Sicherheitsbeauftragte, alle an tieferen Einblicken in IT-Sicherheit aus technischer Perspektive Interessierten
Nützliche Vorkenntnisse	Grundkenntnisse über Betriebssysteme und Rechnerarchitektur
Dauer:	2 Tage
Teilnehmerzahl:	8-12