Buffer Overflow

Projektstand

Jakob Stühn

H-BRS

November 26, 2021

Thema

Theorie hinter Buffer-Overflows

- Stack / Heap
- Instruction Pointer
- Pufferüberläufe

Thema

Buffer-Overflows in der Praxis

- NOP-Slides
- Shellcode
- Vulnerable Functions
- Programmiersprachen

Thema

Buffer-Overflow Demo

- Verwundbares C-Programm
- GNU-Debugger
- Exploit-Entwicklung
- Ausführen auf Serverumgebung

Projektplan

Research

- Theorie
- Prozessoren
- Programmiersprachen
- Angriffstechniken
- GNU-Debugger

Projektplan

Praktischer Teil

- Erproben von Exploit-Techniken an verwundbaren Programmen
- Entwicklung einer verwundbaren Demo Software in C
- Aufsetzten einer Demo-Umgebung (2 Virtuelle Maschinen)
- Entwicklung eines leicht verständlichen Exploit-Script in Python
- Funktionstests der Demo-Umgebung

Projektplan

Dokumentation

- Erstellen einer leicht verständlichen und Präsentation der Demo-Umgebung
- Verschriftlichung der erarbeiteten Inhalte, in Absprache mit Gruppenmitgliedern

Stand des Projekts

Aktuelle Aufgaben

- Abschluss der Funktionstests
- Erstellung der Demo-Präsentation

Stand des Projekts

Probleme

- Herunterbrechen der Demo in leicht verständliche und möglichst kurze Schritte
- GCC-Flags für das Kompilieren des verwundbaren C-Programms

Stand des Projekts

Ausblick

- Verschriftlichung der Inhalte
- Zusammenfügen der von der Gruppe erarbeiteten Ergebnisdokumente