Meeting 06. Oktober - Workshop

Start: 1500
End: 1630

INFO

Nächste Meetings

Donnerstag 13. Oktober: 1030 - 1200
Donnerstag 20. Oktober: 1030 - 1200
Donnerstag 27. Obtober: 1500 - 1700
Donnerstag 03. November: Offen
Donnerstag 10. November: 1330 - 1500 \

Deliverable nächstes Meeting
Draft von Problemdomain mit Lernkonzept(en) und dem Projektplan

Organisatorisches

- Github
- Meeting Minutes
- Projektplan

Dokumentation

- Abstract
  - Für Interessenten --> kann technisch sein
- Management Summary
  - Elevator Pitch
  - Jeder muss es verstehen
- Technischer Bericht
  - Inhalt, damit ein anderer das Projekt weiterführen könnte
- OST Must-Haves
  - PM (Porjekt Mgmnt)
  - Zeit
  - Risiko --> überlegen, was muss in der SA funktionieren (wichtigste Aspekte die eine mögliche Klemme verursachen können) und wie kann man das versichern
  - etc.
- Beilagen
  - Meeting Minutes
  - Source Code (Github Link)
  - 1 x Druckversion (zum lesen)
  - Digital PDF
  - etc

WAS - RE Lab

Ziel: Hacking Lab Integration für den Unterricht (Modulintegration) Landkarte / Roten Faden aufbauen für damit man eine Organisation hat. --> Qualität
--> Gute Tutorials die Zeit benötigen (Besser als schnell durch alles durchgehen) \

- Required Knowhow für Lehrer aufschreiben
- Student im 3. Jahr
- Testpersonen finden
    - Testcases mit Feedback
      --> Feedback designen

Erfahrungen aus den 2 Wochen Vorbereitung

- Zurechtfindung in den Tools wie Ghidra
- Lernen des Programmes hat viel Zeit auf sich genommen

Was muss ein RE können (Problemdomains)

- Networks
- Obfuscation
- VM Erkennung
- Tool Knowhow --> Plugins kennen
- Process Hollowing
- Binaries mit und ohne Hindernissen
- Live vs Dynamic Debugging
- Aufgefrischtes ASM Wissen!

Ideen

- Tutorial mit immer weniger Hilfe. Betti Bossi -> Challenge
- Linux und Windows (Win. nicht nur native sondern auch .NET)
- Strategien anzeigen
- Checkpoint System
- Binary mit Network Traffic beobachten
- Obfuscated Code
    - Knacknüsse für RE
- Welche Software / Tools verwenden
- Source Code zu ASM-Code
    - Wenn die Schüler beides haben können sie Schlüsse ziehen und Verbindungen machen
    - Verschiedenste Möglichkeiten für Aufgaben (x32, x64 etc.)
    - Level von Obfuscation
    - Source Code nicht 1:1 (Passwörter, XOR anders damit Binary anderst ist)
      --> Schüler lernen aus einem Beispiel

- **IMPORTANT** Lernkonzept aufstellen
    - ASM lernen
    - RE Tools lernen
    - Was muss ein RE können / Was ist Vorwissen / Teilschritte die benötigt werden um ein Programm reversen zu können?
      --> Was braucht es alles um die Uebungen lösen zu können

Mini Projektplan

Analyse (Probem Domain) -> Lernkonzept (Was soll das Lab beibringen) -> Was interessiert uns davon? -> Aufgabenkonepte -> Implementationen mit Tests --> Ergebnis