Meeting 20. Oktober

Start: 1010
Ende: 1130

Info

Nächste Meetings
Donnerstag 27. Obtober: 1500 - 1700
Donnerstag 03. November: Offen
Donnerstag 10. November: 1330 - 1500

Deliverables
Students: Exploitation überlegen (vielleicht Mindmap erstellen), GANTT diagram anpassen, Lab intro 2 und 3 erstellen (+- fertig / POC) -> Email notification wenn gepusht (Mittwoch Abend deadline)
Advisor: Sample Courses für RE, ECSC Hacking-Labs freischalten

Präsentation

- Grafik um Active + Passive Network erweitert
  --> Passive (nichts verändert - Wireshark), Active (was verändert)

GANTT Chart

- Finalizing Documentation statt "Documentation"
- Online GANTT chart > Excel

Lab Concepts

- Refresher
  - Vielleicht am Schluss machen damit man weiss was alles braucht im Refresher
  - Binaries aus zukünftigen Labs zusammenstellen
  - ASM
  - Kein C und Python (wenig)
  - Endians
- Intro #1
  - Installationteil
- Intro #2
  - Studenten bekommen Quellcode (Code andere Flag als das Binary)
  - Informationen über den Ablauf der Übung auch ins Concept
- Intro #3
  - Linkback zu vorherigen Übungen gut
- Feedback:
  - Server Teil ist wichtig (nicht nur lokal analysieren sondern auch mit einem docker um remote zu exploiten und analysieren) socat
  - ecsc.hacking-lab.com -> einloggen mit OST daten

    - github.com/hacking-lab -> generator-hl-challenge -> apps -> templates -> binary-c -> services -> server -> run für socat command
    - start docker -> builded file und output in directory -> socat port auf directory
    - Auch exploits einbauen um herausgefundes wissen anzuwenden. (Pwn etc. nutzen)
    - RE ist Mittel zum zweck um Schwachstellen zu finden und auszunutzen
    - Mit lab 2 anfangen zu planen da man da konkret werden muss und aus dem schlussendlich resultierenden paperwork die vorherigen machen.

Planning

- Meetings: Über was haben wir geredet und was nehmen wir uns auf das nächste mal vor. Spezielle Decisions auch hinzufügen
- Exploit teil des RE im MindMap einfzügen (separat oder additiv)

Allgemein

- Einleitung der SA schreiben, für was RE benutzt wird, wer es nutzt, wie man es nutzt etc.
- Construction Phase beginnen -> Von Lab zu Lab planen
- Markdown für Hacking-Lab
    - Haupt MD
    - StepX.md
    - Lösungs MD

Decisions

- Anhand vom Tool Zeit protokollieren -> Kein Estimated also auch nicht erfinden.
- Labs laufend Planen
- Construction Phase jetzt beginnen