Appendix B – Breakdown of the work

🟧 Sandro

🟦 Nils

🟩 Rosalie

All

Table of contents

- 🟧 1 Introduction
- 2 Background
  - 🟧 2.1 Remote Access Trojans / Tools (RAT)
  - 🟧 2.2 DarkComet
  - 🟧 2.3 Volatility
  - 🟧 2.4 VirusTotal
  - 🟧 2.5 YARA Rules
  - 🟦 2.6 Cuckoo Sandbox
  - 🟦 2.7 Virtual Machine Hypervisor
  - 🟩 2.8 Scanning Tools
  - 🟩 2.9 How to recognise DarkComet?
  - 2.10 Ethical & Judicial Aspects
    - 🟦 2.10.1 Analysis
    - 🟩 2.10.2 Scanning
- 3 Design
  - 🟦 3.1 Host System
  - 🟦 3.2 Guest System
  - 3.3 Data Flow
    - 🟧 3.3.1 Reverse Engineering
    - 🟩 3.3.2 Scanning
    - 🟦 3.3.3 Live Analysis
    - 3.3.4 Statistics
  - 🟦 3.4 Automation
  - 🟧 3.5 DarkComet commands documentation
  - 🟩 3.6 Scanning
- 4 Implementation
  - 🟧 4.1 Ubuntu Configuration
  - 🟧 4.2 Cuckoo Configuration
  - 🟧 4.3 Start the Cuckoo System
  - 🟧 4.4 Submit a sample
  - 🟧 4.5 Folder structure
  - 🟧 4.6 Scripts implementation
    - 🟧 4.6.1 Volatility
    - 🟦 4.6.2 Decrypt Network Communication
    - 🟩 4.6.3 Scanning-Scripts
    - 🟧 4.6.4 apscheduler.py
- 5 Experiments
  - 🟧 5.1 Reverse Engineering
  - 🟩 5.2 Scanning
  - 🟦 5.3 Online-Analysen
- 6 Discussion
  - 🟧 6.1 Reverse-Engineering
  - 🟩 6.2 Scanning
  - 🟦 6.3 Live-Analysis
- 7 Conclusion
- Glossary