Zeitplan:

September:

1. Woche: Einführung in Python, Einarbeitung in PE mittels Übersicht, AV-Evasion mit

Veil, Malware mit Poison Ivy erstellen, grundlegende Funktionsweise von AV-

Scannern gelernt, Splitting mit dsplit und Signatur gefunden, einfacher

Crypter für PI.p, Einarbeitung in GIT

PE-Übersicht Headers fertigmachen

1. Woche:

PE-Übersicht 4, 5, 6, 7 fertigmachen

Reverse Engineering von Malware / Windows Rootkits

Assembler

Ghosting

Python

1. Woche: Reverse Engineering von Malware / Windows Rootkits

Assembler

Python

1. Woche: Reverse Engineering von Malware / Windows Rootkits

Assembler

Python

Oktober:

1. Woche: Virtuelle Maschine mit mehreren Virenscannern (wie Virustotal)

Cuckoo Python Framework

1. Woche:
2. Woche:
3. Woche:

November:

1. Woche: Home und Enterprise AV analysieren
2. Woche: Home und Enterprise AV analysieren
3. Woche: Home und Enterprise AV analysieren
4. Woche: Home und Enterprise AV analysieren

Dezember:

1. Woche:
2. Woche:

Dokumentation schreiben, Quellen, …

1. Woche:
2. Woche:

Januar:

1. Woche:
2. Woche:
3. Woche:
4. Woche: