Malware Analysis 6 hours of content | 60 hours of practice | Final Project

1. Malware Research Introduction

- Course goals
- What is a malware
- What is a malware research
- Importance of research
- Malware types in the wild
- Malware triage

2. Malware Lab Environment

- Lab network scope
- Windows 10 lab setup
- Kali Linux lab setup
- Lab optimization
- Flare
- Snapshot Management

3. Anatomy of a process

- What is a process
- Virtual Address
- Physical Address
- OS Loader
- Page table
- Las & Pas
- MMU
- PE Structure
- DOS Header
- NT Header
- File Header
- Optional Header
- Sections
- Exe vs DLL
- Export Address table
- Import Address table
- Must know DLL's
- Functions Fuzzing
- Packers
- Hashing & Fingerprinting
- Host based IOC's
- Network Based IOC's
- Sections
- Textual analysis
- Malware Research Demo
- Hands-on Lab

4. Behavior Analysis

- What is dynamic analysis
- Static Analysis
- Network based analysis - DNS
- Wide Protocols
- Data extraction
- Sysinternals
- Registry monitoring
- Persistence hunting
- File system monitoring
- Process operation breakdown
- Process operation post extract
- Hands-on Lab

5. Signature based detection

- Introduction to Yara rules
- Yara Rules formats
- Yara rules conditions
- Case sensitve strings
- Yara rules automation
- SSMA
- Hands-on Lab

6. Malware Research Project

- Malware Research Reporting
- Malware Labs Project