CMAP Course Syllabus

Malware Analyst Professional - Level 1

Introduction & Lab Setup

- What is Malware and what common types of Malware
- What is Malware Analysis and its purposes
- Types and levels of Malware Analysis (static, dynamic, and code reverse engineering)
- Setting up the Lab (lab architecture overview, setting up Windows Malware analysis lab).
- Optimizing the lab for better and more efficient Malware Analysis
- Deploying Flare-VM
- Deploying REmnux and connecting to InetSim
- Tools of the trade (deployment and overview)

Introduction to Code Reverse Engineering

- The four stages of software development
- Basic C programming examples
- Deploying Visual Studio and compilation tools
- Analyzing compiled assembly code with IDA

Static Malware Analysis

- Identifying common file formats using hex editors and PE parsers
- Malware fingerprinting using calculated hashes
- Using VirusTotal for threat intelligence and multi-AV scanning purposes
- File string extraction and decoding
- Determining obfuscation and Packers
- Inspecting PE header for valuable information and IoC (Indicators of Compromise) gathering
- Classifying malware families and variants
- Packing detection and analysis
- Optimal reverse engineering approaches and methodologies
- Leveraging IDA's Pseudo Decompilation feature
- Approaching and reading function documentation
- Renaming functions/subroutines
- Saving IDA's Reverse Engineering Progress
- Writing your own custom YARA signatures
- Static Reverse Engineering with IDA Pro
- Breaking the FlawedAmmyy RAT into pieces

Dynamic Malware Analysis

- Logging system events using Procmon
- Sniffing and analysis of network traffic using Wireshark
- Execution and analysis of DLL files using Rundll32.exe
- Monitoring Windows API functions using API Logger
- Inspecting process command line arguments using CMD Watcher
- Dynamic Reverse Engineering (debugging) with IDA Pro
- FlawedAmmyy RAT attack flow analysis
- Unpacking/decrypting FlawdAmmyy RAT in-memory runtime payload
- Writing a YARA rule to detect and hunt FlawedAmmyy variants

Malicious Documents Analysis

- Analyzing VBA Macros inside Office documents
- Analyzing a VBA Macros shellcode process injection
- Analyzing PDF exploits leveraging JavaScript

Who should attend?

- IT security professionals
- SOC analysts
- Digital Forensics experts
- Red teamers and penetration testers
- Others with the passion and eagerness to discover and learn new topics