Malware Analysis Fundamentals Course Syllabus (MAF)

This 40-hour, five (5) day course provides a comprehensive overview of the various types of malicious software and their underlying principles through hands-on practical exercises. Students will gain an understanding of static and dynamic analysis techniques and reverse engineering while being able to identify, analyze, and mitigate malware threats effectively.

Through hands-on real-world examples and team collaboration, MAF students will explore use-cases from around the world to practice effective tradecraft and be prepared to operate immediately.

Contact Information

Contact: 443-620-TEAM (8326) Option #2 **or** training@teamworxsecurity.com

Course Description and Course Goals

- Introduction to the history of malware and malware analysis
- Ability to identify types of malware
- Introduction to static and dynamic analysis
- Ability to establish an analysis environment
- Introduction to file structures and analysis
- Introduction to strings and signatures
- Introduction to behavioral analysis
- Ability to produce reporting through the use of templates
- Introduction to open source tooling to support report writing
- Practice executing tools, techniques, and procedures
- Practice presentation and public speaking skills

Module 1

- Introduction to the history of malware and malware analysis
- Exposure to malware definitions and types
- Understanding types of threats
- Ability to recognize vulnerabilities
- Understanding the difference between static and dynamic analysis
- Ability to set up an analysis environment
- Ability to recognize virtualization basics and isolation techniques

Module 2

- Introduction to the purpose and benefits of static analysis
- Exposure to the types of static analysis
- Ability to recognize PE file structures
- Ability to examine file headers and extract metadata and properties
- Understanding of portable executable format and ID key components
- Ability to extract strings and signatures based on detection methods

Module 3

- Introduction to the purpose and benefits of dynamic analysis
- Exposure to the types of dynamic analysis
- Ability to set up a virtual lab environment
- Understanding configuration of virtual machines
- Understanding and maintaining snapshots
- Ability to identify malicious behavior
- Exposure to behavioral analysis through system and network monitoring
- Exposure to dynamic analysis tools

Module 4

- Review of malware best practices
- Practice in basic reporting writing skills with provided templates
- Exposure to open source (OSINT)/publicly available information (PAI) tools
- Practice using OSINT and PAI tools to enhance malware reports writing

Module 5

- Capstone practical analysis of active malware
- Practice communicating actions taken and analytical reports through written and verbal means
- Practice executing tools, techniques, and procedures
- Practice presentation and public speaking skills

Students will Need

A computer with internet access. Students are also welcome to bring any other note taking materials they wish. (some handouts will be provided)

Grading

This course is based on participation within daily discussions and group activities. Students **MUST** be present to do so.

Course Schedule

Course schedules can vary based on customer needs.

Five (5) Day Course Schedule Expectations:

- Daily start time will be 0900 (9 a.m.)
- Daily end time will be between 1600 (4 p.m.) and 1730 (5:30 p.m.)
- Daily lunch break time will be between 1130 to 1300 (1:00 p.m.)
- Daily schedule may flex based on how quickly students are understanding concepts and questions