MALWARE ANALYSIS AND THREAT ASSESSMENT COURSE

This 5-day course will cover the basic of malware analysis from both static and behavioral perspectives. Students will learn to identify, hash, retrieve, and determine what threats and capabilities the malware presents on target hosts.

COURSE OBJECTIVES

- Identify malware types based on static and behavioral analysis.
- Determine malware capabilities and persistence vectors.
- Evaluate potential threat from malware activity on the network.

VERIFICATION

- Students will demonstrate through lab activities and exercises in class how to properly and uniquely identify and categorize malware.
- Students will demonstrate through lab activities and exercises in class how to detect and analyze suspicious and malicious persistence activities on compromised hosts.
- A culmination exercise, consisting of a mixture of malware embedded in software and hosts infected with malware, will evaluate students' adaptation of, and retention of, methodologies taught during class.

CHIRON METHODOLOGY DOMAIN

CYBER PROTECTION PROFESSIONAL™ (CPP)™

DURATION

5 DAYS

RECOMMENDED PRE-REQUISITES

- Familiarity with VMware Player or Workstation
- Familiarity with programming languages
- Familiarity Assembly and Operating Systems

MALWARE ANALYSIS AND THREAT ASSESSMENT COURSE

COURSE SCHEDULE

DAY 1: MALWARE IDENTIFICATION

- Learn how to identify malware based on file characteristics, and how to categorize malware based on programmatic code analysis.

OUTLINE

- Malware Categories
  - Viruses
  - Trojans
  - Worms
  - Bugs
  - Potentially Unwanted Programs (PUPs)
  - Spyware / Adware
  - Bots
  - Remote Access Tools (RAT)
  - Rootkits
- File Metadata Analysis and Code Hashing
  - Standard Hashes
  - Fuzzy Hashes
  - File Section

DAY 2: MALWARE ANALYSIS

- Learn how to rapidly assess and triage malware using static and behavioral analytic methodology.

OUTLINE

- Static Analysis
  - Passive Observables
    - File Type, Size, Entropy
    - Magic File Numbers
    - File Section Strings
    - Common Obfuscation Techniques
    - Function Calls
  - Observation Analysis
- Behavioral Analysis
  - Tracking System Changes
  - Stagers and Dropped Files
  - Observation Analysis

DAY 3: MALWARE PERSISTENCE AND INFECTION VECTORS

- Learn the where and how of malware infection and persistence, as well as command and control, and data exfiltration methods.

OUTLINE

- Windows Operating System
  - Persistence Methods
  - Common Persistence Locations
  - Automated Exfiltration Techniques
  - Initial Infection Vectors
- Linux Operating System
  - Persistence Methods
  - Common Persistence Locations
  - Automated Exfiltration Techniques
  - Initial Infection Vectors

MALWARE ANALYSIS AND THREAT ASSESSMENT COURSE

COURSE SCHEDULE

DAY 4: MALWARE THREAT ASSESSMENT ON TARGET

- Observe malware on target systems and learn how to determine when it can be managed and when it should be avoided.

OUTLINE

- Target Host Operating System
  - System Internals
    - Running Processes
    - Handles and Mutexes
    - File Structure
    - Kernel and Shared Libraries
    - Audit Configurations
    - Data Valuation
    - Accessed Files / Directories
  - Network Activity
    - Port and Protocol Usage
    - Beacon Activity
    - Exfiltration Activity
    - Network Protections / Monitoring
- Malware Author / User Goals
- Risk Assessment / Threat Matrix

DAY 5: CULMINATION EXERCISE

- In a simulated live network, determine what malware is present, and accurately assess whether a host can be safely used or whether a host should be avoided.