TRAINNIX

MEMORY FORENSICS

- 2 Days Programme
- 16 CPE's
- Laptop Required

Memory Forensics Course provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyze captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work & is specially designed for Cyber security professional who are involved in analysing memory as a part of Incident investigations process.

In the first part of the course, the attendees will learn different ways to acquire raw memory for different types of operating systems, identifying and collecting different types of Artifacts.

In the second stage, the attendees will learn how to leverage these collected Artifacts/IOC's for performing Threat Hunting and investigating potential lateral movement.

DETAILED COURSE DESCRIPTION

DAY 1

- Memory Forensics Fundamentals
- Memory Acquisition and Examination
- Memory Analysis Timeline Creation
- Identifying Rogue processes, Process DLLs and Handles in memory.
- Reviewing Network Artifacts, evidence of code injection, check for the signs of Root kits, malwares, acquiring suspicious processes and drivers.
- Advanced Memory Analysis with Volatility.
- Leveraging Volatility to analyze real sample malwares such as Stuxnet, Conficker, BlackEnergy etc.
- Leveraging results/IOC's from memory forensics/analysis for performing Threat Hunting and Detecting Lateral movement

DAY 2

- Introducing Redline for doing Memory Analysis
- Using Redline for auditing and collecting all running processes and drivers from memory, file system metadata, registry data, event logs, network information, services, tasks and web history.
- Leveraging Redline for creating Memory timeline
- Running yara rules against memory image
- Volatility Lab

WHO SHOULD ATTEND

- Incident Response Team Members
- Experienced Digital Forensic Analysts
- Red Team Members,
- Penetration Testers
- Exploit Developers
- Law Enforcement Officers
- Federal Agents and Detectives
- Forensics Investigators

Technical Pre-Requisites

It is highly recommended that the attendees should have good working level knowledge of Windows operating system.

Good knowledge of Networking and TCP/IP concepts, basic network troubleshooting, Basic level knowledge of VMware workstation such as setting up Guest OS, VMware networking.

Additionally, it is advisable to have some prior background and experience in Cyber Security, (but it is not a must have as this course will start from the basics and get into advanced topics and hands-on labs)

Laptop Requirements

- CPU: 64-bit Intel i5/i7 - x64 bit 2.0+ GHz processor or more
- 16 GB RAM or greater, 200 GB of Hard Disk Drive
- VMWare Fusion/Workstation or VMware Workstation player.
- 64-bit version of Windows 7(or above) or Mac OSX
- Install 7-zip on your host OS
- Disable credential guard
- Admin level access to the host operating system as well as guest operating system.
- Wireless 802.11 compatibility