Threat Hunting using Memory Forensics

2 day class

Beginner/intermediate

Memory forensics is a powerful investigation technique used in digital forensics and incident response. With adversaries getting sophisticated and carrying out advanced malware attacks on critical infrastructures, Data Centers, private and public organizations, it is essential for cyber-security professionals to have the necessary skills to detect, respond and investigate such intrusions. Memory Forensics has become a musthave skill for fighting advanced malware, targeted attacks, and security breaches. This training focuses on hunting malware using memory forensics, it introduces you to the topic of Windows internals, and techniques to perform malware and Rootkit investigations. The training covers analysis and investigation of various malware infected memory images(crimewares, APT malwares, Rootkits, etc.) and contains scenario-based hands-on labs to gain a better understanding of the subject.

The training provides practical guidance and attendees should walk away with the following skills:

- What is Memory Forensics and its use in malware and digital investigation
- Ability to acquire a memory image from suspect/infected systems
- How to use open source advanced memory forensics framework (Volatility)
- Understanding of the techniques used by the malwares to hide from Live forensic tools
- Understanding of the techniques used by Rootkits(code injection, hooking, etc.)
- Investigative steps for detecting stealth and advanced malware
- How memory forensics helps in malware analysis and reverse engineering
- How to incorporate malware analysis and memory forensics in the sandbox

Note: Students will be provided with malware-infected memory images, course material, lab solution manual, video demos, and Linux VM.

What Students Should Bring

- Laptop with minimum 6GB RAM and 40GB free hard disk space
- VMware Workstation or VMware Fusion (even trial versions can be used).
- Windows Operating system (preferably Windows 10 64-bit) installed inside the VMware Workstation/Fusion. Students must have full administrator access for the Windows operating system installed inside the VMware Workstation/Fusion.

Fusion. Students must have full administrator access for the Windows operating system installed inside the VMware Workstation/Fusion.

Note: VMware Player or VirtualBox is not suitable for this training. The detailed step-by-step instruction to configure the laptop will be sent to the students a few days before the training.

Course Outine

INTRODUCTION TO MEMORY FORENSICS

- What is Memory Forensics
- Why Memory Forensics
- Steps in Memory Forensics
- Memory acquisition and tools
- Acquiring memory from a physical machine
- Acquiring memory from the virtual machine

VOLATILITY OVERVIEW

- Introduction to Volatility Advanced Memory Forensics Framework

Threat Hunting using Memory Forensics

- Volatility Installation
- Volatility basic commands
- Determining the profile
- Volatility help options
- Running the plugin

INVESTIGATING PROCESS

- Understanding Process Internals
- Process(EPROCESS) Structure
- Process organization
- Process Enumeration by walking the double linked list (pslist)
- process relationship (pstree)
- Understanding DKOM attacks
- Process Enumeration using pool tag scanning (psscan)
- Volatility plugins to enumerate processes

INVESTIGATING PROCESS HANDLES & REGISTRY

- Objects and handles overview
- Enumerating process handles using Volatility
- Detecting malware presence using the mutex
- Investigating registry key using Volatility
- Detecting malware persistence

INVESTIGATING NETWORK ACTIVITIES

- Understanding malware network activities
- Volatility Network Plugins
- Investigating Network connections
- Investigating Sockets

INVESTIGATION PROCESS MEMORY

- Process memory Internals
- Listing DLLs
- Identifying hidden DLLs
- Dumping malicious executable from memory
- Dumping DLL from memory
- Scanning the memory for patterns(yarascan)

INVESTIGATING USERMODE ROOTKITS & FILELESSMALWARE

- Code Injection
- Types of Code injection
- Remote DLL injection
- Remote Code injection
- Reflective DLL injection
- Hollow process injection

INVESTIGATING KERNELMODE ROOTKITS

- Understanding Rootkits
- Understanding API call flow
- Level of Hooking/Modification on Windows
- Kernel Volatility plugins
- Demo Rootkit Investigation

MEMORY FORENSIC CASE STUDIES

- Demo Hunting an APT malware from Memory

Who Should Take This Course:

This course is intended for

- Anyone interested in learning memory forensics and Threat Hunting.
- SOC Analysts
- Incident responders, cyber-security investigators, security researchers, system administrators, software developers, students, and curious security professionals who would like to learn malware analysis.

Trainer Bio

Monnappa K A has over 15 years of experience in incident response and investigation. He previously worked for Microsoft & Cisco as a threat hunter mainly focusing on threat hunting, investigation, and research of advanced cyber attacks. He is the author of the best-selling book "Learning Malware Analysis."He is the review board member for Black Hat Asia, Black Hat USA, Black Hat Europe. He is the creator of Limon Linux sandbox and the winner of the Volatility plugin contest 2016. He is the co-founder of the cybersecurity research community "Cysinfo" (https://www.cysinfo.com). He has conducted training sessions on malware analysis, reverse engineering, and memory forensics at Black Hat, BruCON, HITB, FIRST (Forum of Incident Response and Security Teams), SEC-T, OPCDE, and 4SICS-SCADA/ICS cybersecurity summit. He has presented at various security conferences, including Black Hat, FIRST, SEC-T, 4SICS-SCADA/ICS summit, DSCI, National Cyber Defence Summit, and Cysinfo meetings on various topics related to memory forensics, malware analysis, reverse engineering, and rootkit analysis. He has also authored various articles in eForensics and Hakin9 magazines. You can find some of his contributions to the community in his YouTube channel (http://www.youtube.com/c/MonnappaKA), and you can read his blog posts at https://cysinfo.com
Twitter: @monnappa22