HACKINGPOINT

CHECK POINT

Malware Analysis

2 day class

Beginner/intermediate

This 2-day hands-on training teaches the concepts, tools, and techniques to analyze and to determine the behavior and capability of the malware.
This course will introduce you to the concept of malware analysis and reverse engineering. You will learn to perform static, dynamic, and code analysis to determine the inner workings of the binary.
To keep the training completely practical, it consists of various scenario-based handson labs after each module which involves analyzing real-world malware samples. This hands-on training is designed to help attendees gain a better understanding of the subject in a short span of time. Throughout the course, the attendees will learn the latest techniques used by the adversaries to compromise and persist on the system. In this training, you will also gain an understanding of how to integrate malware analysis techniques into a custom sandbox to automate the analysis of malicious code. After taking this course, attendees will be better equipped with the skills to analyze and respond to malware-related incidents.

Note: Students will be provided with malware samples, malware-infected memory images, course material, lab solution manual, video demos, custom scripts, 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.

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 Outline

INTRODUCTION TO MALWARE ANALYSIS

- What is Malware
- What they do
- Why malware analysis
- Types of malware analysis
- Setting up an isolated lab environment

STATIC ANALYSIS

- Determining File Type
- Fingerprinting the malware
- Extracting strings
- Determining File obfuscation
- Pattern matching using YARA
- Fuzzing hashing & comparison
- Understanding PE File characteristics
- Hands-on lab exercise involves analyzing a real malware sample

DYNAMIC ANALYSIS/BEHAVIOURAL ANALYSIS

- Dynamic Analysis Steps
- Understanding Dynamic Analysis tools
- Simulating services
- Performing Dynamic Analysis
- Monitoring process, filesystem, registry, and network activity
- Determining the Indicators of compromise (host and network indicators)
- Hands-on lab exercise involves analyzing a real malware sample

AUTOMATING MALWARE ANALYSIS

- Custom Sandbox Overview
- Working of Sandbox
- Sandbox Features
- Demo - Analyzing malware in the custom sandbox

HACKINGPOINT

CHECK POINT

Malware Analysis

2 day class

Beginner/intermediate

CODE ANALYSIS
- Code Analysis Overview
- Disassembler & Debuggers
- Code Analysis Tools
- Basics of IDA Pro
- Disassembly using IDA
- Debugging using IDA
- Basics of /x64dbg
- Debugging using x64dbg
- Understanding the API calls
- Call references in IDA and x64dbg

REVERSING MALWARE FUNCTIONALITIES
- Downloader
- Dropper
- Keylogger
- Code Injection
- HTTP backdoor
- Hands-on lab exercise involves analyzing a real malware sample

MALWARE PERSISTENCE METHODS
- Run registry key
- Scheduled Tasks
- Startup Folder
- Service
- Winlogon registry entries
- Image File Execution Options (IFEO)
- Accessibility programs
- AppInit_DLLs
- DLL Search order hijacking
- Hands-on lab exercise involves analyzing a real malware sample

Who Should Take This Course:

This course is intended for
- Anyone interested in learning malware analysis.
- 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