TRAINNIX

ARTIFACTS ANALYSIS FUNDAMENTALS

- 1 Day Programme
- 8 CPE's
- Laptop Required

This course teaches the trainees malicious Artifact analysis fundamentals and various types of analyses. The attendees will be able to learn how to safely execute suspicious code in the controlled environment along with most important security precautions. It teaches the trainees how to perform basic Static and Automatic analysis – what tools can be used, what to look for, what can be found. This workshop gives the attendees the opportunity to use various popular tools during the analyses and let them decide what tools are best suited for different type of analyses. It also cover common malicious software behaviours and patterns – which can be later used to create proper signature.

At the beginning, participants will learn how to use basic static analysis techniques to perform a preliminary study of the sample. Using methods such as strings analysis, portable executable (PE) headers analysis, import address table (IAT) analysis or resources analysis, participants will try to determine some of the Artifacts functionality.

In the later part of the course, participants will perform behavioural analysis in which they will execute samples in a controlled environment. Then they will observe any changes taking place in the operating system such as which processes are created, what changes are made to the file system or the system registry, and if there would be any indicators of rootkit activity. Next, using all gathered information, participants will try to answer how the analysed samples behave after being executed and what would be the indicators of an infected system.
In this way participants will get the opportunity to compare manual analysis techniques with the automatic analysis and learn what are the advantages and disadvantages of using both the techniques.

DETAILED COURSE DESCRIPTION

- Malware analysis fundamentals
- Various approaches to malware analysis
- Overview of different types of analysis tools such as Static analysis tools Dynamic analysis tools, Network analysis tools, Automatic analysis tools

WHO SHOULD ATTEND

- Network security professionals and incident responders
- Threat Hunters
- SOC Analyst
- Experienced Digital Forensic Analysts
- Information Security Professionals

Static analysis

- Sending sample to the analysis.
- Detecting packers and protectors
- Strings extraction and analysis
- PE structure and headers analysis
- Import table analysis
- PE resources analysis
- Searching for embedded objects

Behavioural analysis

- Executing malware sample
- Process Explorer analysis
- Regshot analysis
- Process Monitor analysis
- Searching for Rootkit artifacts

Automatic/Dynamic analysis

- Sending samples to Cuckoo
- Analysing Cuckoo Sandbox results
- Static Analysis results from Cuckoo Sandbox
- Behavioural Analysis results from Cuckoo Sandbox
- Network Analysis results from Cuckoo Sandbox
- Analysing list of dropped files from Cuckoo Sandbox
- Registry analysis results from Cuckoo Sandbox

Technical Pre-Requisites

- This course is designed for Cyber Security professionals who are involved in doing quick assessment of encountered new threats, especially those associated with suspicious executable files.
- It is highly recommended that the attendees should have a good working level knowledge of Windows operating system.
- They should have 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
- 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
- Admin level access to the host operating system as well as guest operating system