Malware Analysis

Course 71590 – 40 Hours

Overview

Malware Analysis is the study and close examination of malware to understand its origins, purpose, and potential impact on the system. Malware analysts accomplish their tasks by using various tools and expert-level knowledge to understand what a piece of malware can do and how it does it. This course provides participants with the practical skills and knowledge to analyze malware and exposes them to a critical set of tools required for their tasks.
The course helps prepare for the certification exam GREM (SANS).

On completion, Delegates will be able to

- Malware analysis using both Dynamic and Static analysis methods
- Assembly language to examine malware
- Reverse engineering malware using various tools
- The first glimpse into Windows kernel

Who should attend

- Cybersecurity practitioners
- Cyber forensics analysts
- Security engineers/researchers
- Incident responders
- Junior malware analysts or reverse engineers
- Software developers
- IT security administrators

Prerequisites

Advanced knowledge of:

- Linux
- Network Forensics (Course 71586) or Windows Forensics (Course 71585)

Course Contents:

Module Title	Description
Module 1: Introduction to Malware Analysis In the first module, students will study different types of malware and see how they operate, understand how the anti-virus works, and eventually develop an idea of approaching a malicious file and where to find it.	▪ **Introduction to Malware Analysis** ○ Malware Analysis Definitions ○ Types of Malware ○ Different Behaviors of Malware Types ○ Security Mechanisms ○ How the Anti-Virus Works ○ Understanding PE Format ○ Hash and File Identification ○ Windows Libraries and Processes ○ Windows APIs ○ Setting Up a Safe Environment for Inspecting Malware ▪ **Extracting malware from data segments** ○ Network PCAP file ○ Volatile Memory (RAM) ○ Basics of Volatile Memory Malicious Activity Research
Module 2: Basic Static Analysis Basic static analysis allows the malware-researcher to inspect the influences of malware on the system while it is in a static stage, that is, in code format. This phase is critical for collecting information about the malware for more advanced stages of the research.	▪ **Basic Static Analysis** ○ Security Concerns ○ First Analysis with Strings ○ PE file Sections ○ Information Gathering from PE ○ Analyzing Program Dependency Libraries ○ Resources Section Anomaly ○ VirusTotal ○ Database of File Hashes ○ Writing Static Analysis Report
Module 3: Basic Dynamic Analysis Basic Dynamic Analysis is the initial method of inspecting and analyzing malware. Students will activate the malware in a protected sandbox environment during this stage and analyze its effects on the system. Various tools for malware analysis will be introduced and used by participants during this module.	▪ **Basic Dynamic Analysis** ○ Organize and Isolate your Environment ○ New Malware System ○ Snapshot System ○ Analyzing Processes ○ Registry Analysis ○ Monitoring Registry Changes ○ Analyzing Autoruns ○ Network Traffic Monitoring with Wireshark ○ Faking Network Traffic and Configure Proxies ○ DNS Monitoring ○ Simulating Internet Services ○ Analyzing Findings

Module 4: Assembly x86 This module will introduce Assembly language basics closest to the binary computer language that humans can read. Familiarization with Assembly will allow students to gain a closer insight into what lies at the base of the malware's code and how it was meant to operate when activated and is an entry ticket into the world of reverse engineering.	▪ **Assembly Language Basics** ○ x86 Processor Architecture ○ Understanding Buses and Data Traffic ○ Syscalls Table ○ Number and Character Representation ○ Basic Assembly x86 Programming