Syllabus

Malware Analysis

CYBERIUM ARENA
-SIMULATOR-

Description

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).

Target Audience

The course targets participants with a strong foundation in the forensics world and wishes to upgrade their skills into the malware analysis world.

Pre-requisites

Linux
Forensics

Objectives

- Malware analysis using both dynamic and static analysis methods
- Learning the Assembly language to examine malware
- Understanding malware using various tools

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 antivirus works, and eventually develop an idea of approaching a malicious file and where to find it.

Introduction to Malware Analysis

- Types of Malware
- Memory Analysis
- Security Mechanisms
- Understanding the PE Format
- Windows Libraries and Processes
- Windows APIs

Setting Up a Safe Environment for Inspecting Malware

- Building and Configuring Virtual
- Machine Malware Analysis Tools

Extracting Malware from Data Segments

- Network PCAP file
- Volatile Memory
- Malicious Activity Research

Module 2: Basic Analysis

Basic static analysis and basic dynamic analysis allow the malware-researcher to inspect malware influences on the system while it is in static and dynamic modes. This phase is critical for collecting information about the malware for more advanced stages of the research.

Basic Static Analysis

- PE File Sections
- Information Gathering from PE
- Analyzing Program Dependency Libraries
- Resources Section Anomaly
- Database of File Hashes

Basic Dynamic Analysis

- Identifying Virtual Machines
- Searching for Ports
- Testing Network Traffic
- Snapshot System
- Analyzing Processes
- Registry Analysis
- DNS Monitoring
- Simulating Internet Services
- Analyzing Findings

Module 3: Advanced Dynamic Analysis

Advanced dynamic analysis is the stage to inspect and analyze malware at a higher level. Students will learn to use debuggers and analyze the malware.

Advanced Analysis

- Understanding Debuggers
- Running Malware in OllyDbg
- Running Malware in Windbg

Module 4: Advanced Static Analysis

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

Disassembler

- Using IDA
- IDA Features
- Analyzing Malware with IDA Pro