CYBERIUM ARENA

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 using various tools and expert-level knowledge to understand what a piece of malware can do and how it does it.

MALWARE ANALYSIS

Module 1: Intro to Malware Analysis

Basic Static Analysis examines a program's code without executing it, enabling early identification of potential threats. Basic Dynamic Analysis refers to the examination of a program during its execution, providing insights into its real-time behavior and potential vulnerabilities.

Basic Static
Types of Malwares
Understanding the PE Format
Windows Libraries and Processes
Setting a Sandbox
Building and Configuring Virtual Machine
Malware Analysis Tools
Basic Dynamic
Identifying Virtual Machines
Searching for Ports
Testing Network Traffic
Analyzing Processes
Registry Analysis
Simulating Internet Services

Module 2: Malware Payloads

Malware Payloads refers to the part of the malware that performs malicious actions, such as data exfiltration or system damage. Understanding payloads helps in assessing threats and strategizing defenses. On the other hand, YARA is a powerful tool used for creating descriptions to identify and classify malware based on textual or binary patterns, enhancing malware detection capabilities.

Payloads
Different Spreading Methods
Viewing Malware Activities
Executing Persistence
Linux Malware Overview
Detection
YARA Rules
Working with IMPHash

Module 3: General Analysis

Analyzing Network Connections involves monitoring and reviewing network traffic to detect anomalies or potential threats. Identifying Malicious Activities equips learners to recognize unusual system behaviors indicating potential security breaches. Memory Analysis is the study of data in a system's memory, often used to detect sophisticated malware or investigate incidents in digital forensics.

Analyzing Network Connections
Extracting Files
Analyzing HTTP and HTTPS
Identifying Malware Downloads
Identifying Malicious Activities
Malware Attacks
Memory Analysis
Identifying Malware
Extracting Malware

Module 4: Advanced Analysis

Assembly Language Basics provides a groundwork understanding of low-level programming critical for tasks like reverse engineering. The Disassembler component allows the translation of machine language into assembly code, enabling better comprehension of a program's function. Advanced Dynamic Analysis involves studying programs in execution, a valuable method for understanding complex malware behavior.

Assembly Language Basics
x86 Processor Architecture
System calls
Basic Assembly x86 Programming
Disassembler
Analyzing Malware with IDA Pro
Advanced Dynamic Analysis
Understanding Debuggers
Running Malware in OllyDbg

NX Defense | LEVEL: 6 | DURATION: 40h