CYBERIUM ARENA

Description

This reverse engineering program, specifically tailored for the modern cyber expert. This meticulously designed program delves deep into the analysis of both Windows and Linux executables. From the foundational principles of binary structures to the hands-on techniques of real-world software threat mitigation, participants will be equipped with a robust skill set, mastering a plethora of tools and strategies that ensure proficiency in deciphering, understanding, and counteracting software vulnerabilities and malicious threats.

REVERSE ENGINEERING

Module 1: Reverse Engineering

Begin with a deep dive into the foundational pillars of reverse engineering, understanding its pivotal role in today's cybersecurity landscape. Participants will set up a dedicated lab environment, ensuring a hands-on approach from the get-go. The module will also introduce the core concepts of binary structures, file formats, and the nuances of various assembly languages, laying the groundwork for advanced exploration.

Foundations of Reverse Engineering
Setting Up the Lab
Essential Tools and Software
Isolating the Lab and Ensuring Data Integrity
Introduction to Executables and Libraries
Understanding Binary Structures and Headers
Assembly Language Primer
Basics of x86, x64, and ARM

Module 2: Static/Dynamic Analysis

Transition into the world of code analysis, both from a static perspective, where code is dissected without execution, and dynamically, observing software behavior in real-time. This module is designed to provide participants with a thorough understanding of renowned reverse engineering tools and methodologies. Special emphasis will be placed on techniques like unpacking and deobfuscation, crucial for deciphering complex and obfuscated software constructs.

Introduction to Code Disassembly
Understanding Control Flow Graphs
Dynamic Analysis Essentials
Setting up a Debugger
Breakpoints, Stepping, and Memory Inspection
Monitoring System Calls and Network Activity
IDA Pro: Features, Shortcuts, and Plugins
Ghidra: Open-source Powerhouse
OllyDbg, GDB, and Radare2
Unpacking and Deobfuscation
Introduction to Packed and Obfuscated Code
Techniques and Tools for Unpacking

Module 3: Advanced RE

This module offers a comprehensive exploration of both Windows and Linux operating systems, focusing on their unique challenges and threats. Participants will analyze platform-specific malware, understand system and API calls, and dive into the complexities of kernel-level reverse engineering, ensuring a holistic understanding of both platforms.

Windows Deep Dive
Understanding Windows API Calls
System Libraries and Their Significance
Malware Analysis Techniques
Windows Kernel Reverse Engineering
Linux Deep Dive
Linux System Calls Monitoring
Shared Libraries
Linux Malware and Rootkits Detection
ELF Binary Analysis Techniques

Module 4: Real-World RE

The module will introduce the art of vulnerability identification from software patches, offering insights into the world of software updates and their security implications. Additionally, a significant portion will be dedicated to the ethical dimensions of reverse engineering, ensuring participants are well-versed in the moral and legal boundaries of their expertise.

Practical Scenarios
Analyzing Real-world Malware Samples
Bypassing Protections
Introduction to Software Patches
Identifying Vulnerabilities
Case Studies: Famous Vulnerabilities
Efficiency through Automation

NX Defense | LEVEL: 7 | DURATION: 40h