SDA.ACADEMY
Cybersecurity training

THINKCYBER

Syllabus

Exploit Development Advanced

CYBERIUM ARENA

-SIMULATOR-

Description

In this course, students will further deepen their knowledge and understanding of exploit research and development. This comprehensive course is designed to turn the students into high-level security experts. The participants will learn how to find critical vulnerabilities everywhere in the platforms and exploit them.

The course helps prepare for the certification exam SEC760 (SANS).

Target Audience

This course is aimed at cyber experts interested in studying one of the most prestigious topics in the field of cyber, developing vulnerability exploitation, and understanding how researchers find security holes and create their code for exploiting vulnerabilities.

Pre-requisites

Networking

Penetration Testing

C

Assembly

Objectives

- Discovering different levels of vulnerabilities, including zero-day vulnerabilities
- Understanding the methods of attacks
- Infrastructure and system defense
- Become familiar with APT and attacks
- Understanding modern security mechanisms

Module 1: Buffer Overflow Attacks

This module will introduce participants to the world of exploit development, explain the basic rules, what needs to be focused on, and create a neat and professional work process. This module will show the basic techniques of binary exploitation.

Anatomy of a program in memory

- Process Memory Organization
- Memory stack
- Buffer Overflow Concepts and Definitions
- Brief on Assembly Registers and Data Organization

Stack overflow

- The Stack Variables
- Environment Variables
- Overwriting Function Pointers Stored on the Stack
- Segmentation Fault Error
- Understand Pointers
- System instructions and OP Codes
- Executing '\xcc' Instruction
- Find Executable Crash-Address
- Crashing Executables with Programming
- Allocate Buffer Size
- Allocate Shellcode Size
- Stack Common Defense Mechanisms
- Working with NOP
- Find JMP Instructions in the Memory
- Writing POC Code

Format strings vulnerability

- Strings Leakage
- Modify the Execution Flow of Programs
- Modify Arbitrary Memory Locations
- Specific Values Assignments
- Writing Larger Data to the Process
- Redirecting Execution in a Process

Module 2: Advanced Buffer Overflow Attacks

In this module, students will learn about buffer overflow capabilities and present advanced and widely accepted techniques in the world of binary exploitation.

Heap Overflow

- Heap Memory Section
- Heap Structure and Functionality
- Influence the Code Flow
- Hijacking in Data Overwrite
- Heap Pointers
- Heap Metadata
- 'Dlmalloc' to Change Program Execution

Advance overflow techniques

- Converting Strings to Little Endian Integers
- Convert Binary Integers into ASCII Representation
- Working with 32-bit Unsigned Integers
- Remote Blind Format String
- Remote Heap Overflow Attack
- Heap Overflows using VEH
- Heap Overflows using the UEF

Module 3: Linux Executables Exploitation

In this module, students will learn to analyze the misconfigured C-code program to take advantage of and write exploitation code to manipulate the system.

Analyzing C Code Programs

- SUID Files
- Permissions
- Race Conditions
- Shell Meta-Variables
- $PATH Weaknesses
- Scripting Language Weaknesses
- Binary Compilation Failures
- Program That Allows Arbitrary Programs to be Executed
- Manipulating Crontab Instructions
- Bypassing Restriction Code of File Read Permissions
- Exploiting Directory Permissions
- Escape Restricted Shells and Environments
- Binary Processes Standard Input and Executes a Shell Command
- Exploit Local Network Services