SDA.ACADEMY
Cybersecurity training

THINKCYBER

Syllabus

Exploit Development

CYBERIUM ARENA

-SIMULATOR-

Description

During this course, participants will learn programming languages and shellcode writing. They will acknowledge program structure and execution patterns and find vulnerabilities and exploit in programs and codes to control target systems and applications. It also covers how to write shellcodes, programs, tools, and essential skills for advanced penetration testers and software security professionals.

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

Objectives

- Understanding the methods of attacks
- Discovering different levels of vulnerabilities, including zero-day vulnerabilities
- Infrastructure and system defense
- Become familiar with APT and attacks that happened in recent years

Module 1: C Programming Crash Course

In this module, students will learn a course that will speed up (-language programming capabilities to acquire the necessary writing shellcode skills.

C Programming Fundamentals

- Variables
- Input and Output
- Keywords and Operators
- Expressions and Statements
- Control Flow
- The C Preprocessor
- Functions
- Pointers
- Code Structures
- Using C Libraries
- Memory Allocation

Module 2: Assembly x86

Students will acquire the machine language assembly experience in this module to become familiar with shellcode codes and write one by themselves.

x86 Processor Architecture

- Understanding Buses and Data Traffic
- Syscalls Table
- Number and Character Representation
- Basic Assembly x86 Programming
- Standard Output
- Registers
- Variables and Reserves
- Strings in Assembly
- Working with Numbers
- Jumps and Flags

Module 3: Writing Shellcodes

Shellcode is a set of instructions that executes a command in software to take control of or exploit a compromised machine. In this module, students will understand how shellcode is built, how it is used, and to write it using conventional methods.

Background Information

Processor Registers Structure

Understanding Upper and Lower Data Block

Syscalls with Arguments

Zero Out a Register

Windows Calling Convention

Shellcode Tools

Find the DLL Base Address

Find the Function Address

Call the Function

Write the Shellcode

Test the Shellcode

Linux Shellcoding

Loading Addresses

Spawning a Shell

Windows Shellcoding

Using Sleep Function

Writing Message

Adding an Administrative Account

Printable Shellcode