SDA.ACADEMY
Cybersecurity training

THINKCYBER

Syllabus

Windows Exploitation

CYBERIUM ARENA

-SIMULATOR-

Description

Microsoft Windows is one of the most popular operating systems ever used. This operating system can be found on any device, such as computers, phones, banking machines, and many more. In this training, students will learn about the Windows operating system's advanced hacking techniques. Students will also experience both offensive and defensive methods; students will learn the latest hacking methodologies.

The course helps prepare for the certification exam OSEE (Offensive Security).

Target Audience

The course targets penetration testers and security experts interested in upgrading their cyber knowledge and capabilities in the Windows operating system environment.

Pre-requisites

Linux
Penetration Testing

Objectives

- Learning advanced attack methods
- Using Windows API
- Using PowerShell

Module 1: Windows Management Instrumentation (WMI)

This module will explain and expand on the use of Windows Management Instrumentation. Students will learn how the core management process is accomplished and use WMI to manage both local and remote computers on the LAN network.

WMI Architecture

- Using WMI Methods
- Working with Remote Computers
- Information Gathering
- Active Directory Enumeration
- Lateral Movement
- Storage Information
- Command Execution
- WMI Common Events
- Detection with WMI

Module 2: Offensive PowerShell

PowerShell is a built-in shell, available on every supported version of Microsoft Windows, and provides incredible flexibility and functionality to manage the Windows system. In this module, students will learn various techniques to use PowerShell as a Red-Team tool in the Windows environment and understand and leverage the PowerShell platform's capability to maintain access.

Introduction to PowerShell Scripting

- About PowerShell
- Using ISE, help system, cmdlets, and syntax of PowerShell Scripting Basics
- Working with Pipeline, Files, Functions, Objects, Jobs, and Modules
- Improving Performances
- Executing Policies with Scripts
- Command Injection

PowerShell as Offensive Tool

- Gathering Information about the Network
- Vulnerability Scanning and Analysis
- Avoiding Detection
- Tools Written/Integrated with PowerShell
- Brute Forcing
- Client-Side Attacks
- Using Existing Exploitation Techniques
- Porting Exploits to PowerShell- When and How
- Human Interface Device
- Getting Foothold on the System
- Use Management Tools to Attack Systems
- Writing Shells in PowerShell
- Pivoting to other Machines using PowerShell

Module 3: Windows Application Programming Interface (API)

API is a set of functions that allows applications to access data and interact with external software components, operating systems, or microservices. This module will focus on Windows API attack capabilities.

Windows API Overview

Windows Internals
Drivers
Memory
Threads
Process Listing Syscall
System Activity in Windows Kernel
Dumping DLL
Detect Remote Thread Injection
Enumerating the Structure
Tokens and Privileges
Reading Process Memory