Welcome
to
Windows Kernel
Internals, Programming & Rootkits
Training

Developed and Presented by :

CodeMachine

Security Research, Development and Training

www.codemachine.com
twitter.com/codemachineinc
facebook.com/codemachineinc

Introduction

- T.Roy (troy@codemachine.com)
  - 25 years experience in system software development
  - Author, instructor, consultant & founder of CodeMachine
- CodeMachine
  - Security Research, Development and Training Company
  - Custom software development services
    - Filter Drivers, Networking, Storage & File Systems
    - Windows, Linux and Internet of Things (IoT)
  - Onsite and online training courses
    - Windows Internals for Malware Analysts
    - Windows Kernel Internals for Security Researchers
    - Windows Kernel and Filter Driver Development
    - Windows Kernel Exploitation and Rootkits
    - Windows Kernel Debugging and Memory Dump Analysis
    - IoT Internals, Programming and Debugging (Linux on ARM)

Kernel Internals Course Goals

- Understand the behind the scenes working of the Windows kernel with emphasis on
  - Components
  - Algorithms
  - Data Structures
  - Debugger Commands and their output
- Follow along labs with intensive usage of WinDBG to drill into the internals
  - Pre-captured memory dumps
  - Live VM

Kernel Programming Course Goals

- Understand the interfaces provided by the Windows kernel and their usage in developing kernel drivers
  - Functionality
  - Programming Model
  - APIs & Parameters
  - Use Cases
  - Common Pitfalls
- Labs involve coding, building, deploying, testing and debugging Windows kernel drivers
  - Drivers are developed based on existing templates
  - Drivers are tested in a virtual machine

Kernel Rootkits Course Goals

- Understand the interfaces and mechanisms exploited by kernel mode software from an offensive (rootkits) and defensive (anti-malware) perspective
- Understand the security mitigations added to Windows to thwart malware and how they can be bypassed
- Extensive hands-on programming and debugging labs
    - Labs are performed on Live VM

Course Pre-requisites

- Good understanding of Windows OS concepts like process, thread, virtual memory, file system, registry, interposes communication and synchronization etc.
- Good command of C programming language including structures, pointers, arrays, parameters and locals variables
- Understanding of x86/x64 compiler calling convention and stack layout
- Ability to read x86/X64 assembler and map to high level language constructs

Course Directory and File Manifest

- C:\course on the host system
- C:\transfer on the target VM, mapped as Z:\ on host

Directory	Content Description
refs	Publicly available reading material.
source	*.labs.zip Contains source code templates for hands-on labs. *.sols.zip Contains complete source code for hands-on labs. *.src.zip Sample driver and application code for demos.
runtime	Debug C Run Time DLLs for hands on labs. These files must be copied to the guest VM.
tools	Collection of publicly available tools for use during the course. These files must be copied to the guest VM.
dumps	Memory dumps from different versions of Windows for demos.
rootkits	Memory dumps, process monitor logs for rootkit analysis.
scripts	Scripts for configuring VM. These files must be copied to the guest VM.
dbgexts	32 and 64 bit version of WinDBG extension DLLs for demos.

Logistics

- Timing
  - Start : 9:00 AM
  - Finish : 4:00 PM - 5:00 PM
  - 10 minute short breaks (every hour on the hour)
  - 1 Hour lunch break (12:30 PM – 1:30 PM)
- Cell Phones OFF or in Vibrate Mode
- Make yourself comfortable, relax and enjoy the class
- Solutions to hands-on labs will be provided at the end of the course

Remember – If you have a question you must ask it !