Montrehack | Anti-Debugging

Introduction to Common Windows Techniques

Twitter @alxbl_sec | **Keybase** @alxbl

Quick Start | Challenge Information

URL: https://segfault.me/ctf/debugme.exe

Flag Format: FLAG-{[\w]+}

No Validation Page. You'll know when you have the flag.

Flag is **in memory**. You must read it from there. It will not be printed.

Intended Solution: Bypass the anti-debug checks and break to read the flag.

Side-Channels: Feel free to show them off :)

Anti-Debugging | One Sentence Definition

Anti-debugging is the act of leveraging behavior that differs depending on whether a debugger is watching the program execution or not to determine its presence and alter execution behavior to prevent analysis and hide the real intent of the program

Motivation | Why Bother?

- Prevent (Dynamic) Reverse-Engineering
- Detect the Presence of a {Researcher,Hacker,Sandbox,...}
- Protect Intellectual Property
- Hide Malicious Functionality
- Hide CTF Flags :)

Behavior | Some Ideas

- Exceptions that the Debugger won’t Rethrow
- Internal Structure Flags Altered by the Debugger
- Stack Address Range
- Delay from Manual Stepping
- …
- Anything you can Think of

Bypassing | Common Techniques

- Patch Instructions to always Fail or always Pass
- Suspend Watchdog Threads
- Patch Data to have the Pre-Detection Result
- Re-implement Desired Behavior and Replace Code
- Emulate Program Code
- Static Analysis

Bypassing | Persistence

Changes are not persisted and must be repeated every session… tedious!

- **Loader**: Launches Target Suspended, Applies Patches, then Resumes.
- **Patch File**: Statically Modify the Binary on Disk. Permanent. Complicated.
- **Hybrid**: A Mix of the Above Techniques

This Workshop: Persistence is not the goal.

(But do take a look at x64dbg’s patching support.)

Challenge | Details

URL: https://segfault.me/ctf/debugme.exe **Slides:** https://segfault.me/ctf/slides.pdf

x64dbg Cheatsheet

; Comment

: Label @ current address

Alt+; Label @ Call/JMP

* Return to instruction pointer

Shift-F Selection into function

G Graph current function

Win64 Calling Convention

call(rcx, rdx, r8, r9, [stack...])

Googling API Calls:

MSDN ExitProcess

Flag Format: FLAG-{[\w]+}

Good Luck ; Have Fun!

Challenge | Solutions & Demo

Level 1: Patch out IsDebuggerPresent to always return false

Level 2: Convert the conditional jump to an unconditional jump

Level 3: Patch out the annoying thread and the breakpoint code to fallthrough

Level 4: Patch the pointer to the key function to avoid the access violations

Level 5: Patch the key into the key table (or in the TLS mov instruction)

Challenge | Additional Resources

On Github (https://github.com/alxbl/montrehack-antidbg)

- Source Code
- Binary
- Symbols
- x64dbg Database

Challenge Write-up on my Blog Soon™