CORELAN HEAP EXPLOIT DEVELOPMENT MASTERCLASS FOR WINDOWS (CORELAN 2)

DESCRIPTION

Level: Advanced

Duration: 4 days

Instructor: Peter Van Eeckhoutte

The Corelan "HEAP" exploit development MASTERCLASS is a fast-paced, mind-bending, hands-on course where you will learn advanced heap manipulation and exploit development techniques from an experienced exploit developer.

During this 4-day class, students will have the opportunity to learn how to write heap exploits for the Windows platform, using Windows 7, Windows 10, and Windows 11 as examples, with a primary focus on learning and applying generic techniques that can be applied to other operating systems and heap implementations.

We will discuss the differences between Windows 7 and Windows 10/Windows 11, and explore previously undocumented techniques to achieve necessary exploitation primitives in Windows 10 and Windows 11. The trainer will share his "notes from the field" and various tips & tricks to become more effective at writing exploits.

The current edition of the course is based on Windows 11/10 and Windows 7 (As the Windows 10/11 Heap Manager contains additional mitigations, we use Windows 7 first to teach the basics, and then use Windows 11/10 later on). Furthermore, this course contains an intro to x64 exploitation (stack & heap), providing you with the required fundamentals to get started with x64 exploitation yourself.

During all of our courses, we don't just focus on techniques and mechanics, but we also want to make sure you understand why a given technique is used, why something works and why something doesn't work.

MODULE 0x00 – ASLR & DEP Refresher

1. Bypassing ASLR
2. Bypassing DEP

MODULE 0x01 – WinDBG classic / WinDBGX

1. WinDBG classic and WinDBGX fundamentals
2. Symbols
3. Breakpoints, logging breakpoints
4. Using WinDBG(X) to explore Windows Heap datastructures in Windows 7, Windows 10 and Windows 11

MODULE 0X02 – Windows Heap Management

1. Terminology & building blocks
2. Windows 7 Heap, Windows 10 (and Windows 11) Heap (“NT” and “Segment” heap)
3. Front-End-Allocator and Back-End-Allocator
4. Differences between Windows 7 & Windows 10 / Windows 11
5. Heap manipulation and exploitation primitives
6. Advanced BEA feng shui
7. Learn how to do your own heap related research, what to look for

MODULE 0X03 – Heap Spraying

1. Basic mechanisms
2. Data & object spraying
3. Precise heap spraying

MODULE 0X04 – Heap Exploitation

1. Use-After-Free
2. Linear & non-linear overflows / controlled write
3. Double Free
4. Type confusion
5. Use of uninitialized memory

6. Crash analysis & classification
7. Memory leaks / Information Disclosure
8. Heap Manipulations and heap primitives
9. How to avoid heap sprays
10. How to get better at finding bugs

MODULE 0X05 – Intro to x64 heap exploitation

1. x64 processes, memory map, registers
2. Functions & calling conventions
3. Structured Exception Handling
4. ASLR
5. Stack Buffer Overflows
6. Heap exploitation primitives on x64

MODULE 0X06 – What's next

1. Overview of memory protection evolutions

PREREQUISITES

Students should be:
- able to read simple C code and simple scripts
- familiar with writing basic scripts using python/ruby/…
- ready to dive into a debugger and read ASM for hours and hours and hours
- ready to think out of the box and have a strong desire to learn
- fluent with managing Windows / Linux operating system and with using VMware workstation/VirtualBox
- familiar with using Metasploit

TARGET AUDIENCE

- Information Security Specialists
- Pentesters
- Red Teamers
- Reverse Engineers
- Malware Analysts
- Developers
- Information Security Enthusiasts
- Members of a Security Department
- Anyone interested in exploit development

REQUIRIMENTS

- A laptop (no netbook) with VMware workstation/fusion/VirtualBox and enough processing power and RAM (we recommend a minimum of 8Gb of RAM) to run up to 2 virtual machines at the same time. The use of a 64bit processor and a 64bit operating system on the laptop will make the exercises more realistic.
- 2 Virtual machines installed: Windows 11/Windows 10 (or Windows 7 SP1) no patches, Kali Linux (fully up-to-date).
- The students will receive the exact installation instructions after registration, about a week before class begins, so don't start installing the VMs yet.
- All required tools and applications will be provided during the training or will be downloaded from the internet during the training.
- The students must have full administrator access to all machines. They must be able to install and remove software, and they must be able to disable and/or remove firewall/antivirus/… when necessary.

SKILLS LEARNED

In the end of the course, the student will be able to:

- Understand the fundamentals of exploit development for Windows Binaries
- Debug Windows applications
- Read and understand existing exploits
- Write reliable exploits for Windows applications
- Get comfortable with exploit writing
- Know what shellcode is
- Master the concept of stack-based buffer overflow for Windows
- Use Egghunter technique
- How to deal with bad characters
- Write exploit for the Metasploit Framework
- Understand Windows Exploit Protections like ASLR and DEP
- Bypass ASLR
- Bypass DEP
- Understand and use ROP technique to bypass DEP
- Understand de fundamentals of x64 stack-based exploitation
- Think out-of-box to solve problems/challenges