EXPERT LEVEL STACK-BASED EXPLOIT DEVELOPMENT FOR WINDOWS (CORELAN 1)

DESCRIPTION

Level: Beginner to Intermediate

Duration: 4 days/40 hrs

Instructor: Peter Van Eeckhoutte

This four-day Bootcamp introduces both basic and advanced techniques from Peter of Corelan. This course is a truly unique opportunity to learn both basic & advanced techniques from an experienced exploit developer. During this course students will be able to learn all ins and outs about writing reliable stack based exploits for the Windows platform. The trainer will share his "notes from the field" and various tips & tricks to become more effective at writing exploits.

We believe it is important to start the course by explaining the basics of stack buffer overflows and exploit writing, but this is most certainly not "your average" entry level course. In fact, this is a true bootcamp and one of the finest and most advanced courses you will find on Win32 stack based exploit development.

This hardcore hands-on course will provide students with solid understanding of current stack based exploitation techniques and memory protection bypass techniques. We make sure the course material is kept updated with current techniques, includes previously undocumented tricks and techniques, and details about research we performed ourselves. Combined with the way the course is built up, this will turn this class into a truly unique experience. **Sign up for this class and learn directly from the author of mona.py**

The current edition of the course is 100% based on Windows 11 / Windows 10 and contains an introduction to x64 stack-based exploitation.

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 – The x86 environment

1. System Architecture
2. Windows Memory Management
3. Registers
4. Introduction to Assembly
5. The stack
6. Running 32bit applications on a 64bit OS (wow64)

MODULE 0x01 – The exploit development lab environment

1. Setting up the exploit developer lab
2. Using debuggers and debugger plugins to gather primitives
3. Learn how to use mona.py directly from the author of mona.py

MODULE 0X02 – Stack Buffer Overflows

1. Stack Buffers
2. Functions
3. Saved return pointer overwrites
4. Stack cookies
5. Structured Exception Handlers

MODULE 0X03 – Egg hunters

1. Using egghunters
2. Egg hunters in a WoW64 environment

MODULE 0X04 – Reliability++ & Reusability++

1. Finding and avoiding bad characters
2. Creative ways to deal with character set limitations

MODULE 0X05 – Metasploit framework Exploit Modules

1. Writing exploits for the Metasploit Framework
2. Porting exploits to the Metasploit Framework

MODULE 0X06 – ASLR

1. Bypassing ASLR

MODULE 0X07 - DEP

2. Bypassing NX/DEP
3. Return Oriented Programming / Code Reuse (ROP)

MODULE 0X08 - Intro to x64 stack based exploitation

1. x64 processes, memory map, registers
2. Functions & calling conventions
3. Structured Exception Handling
4. Stack buffer overflows
5. ROP
6. Shellcode

PREREQUISITS

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