CENTER FOR CYBER SECURITY TRAINING

Corelan Bootcamp Exploit Development

Abstract

This "**BOOTCAMP**" 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 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 x86 (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.

The new 2019 edition of the course is 100% based on Windows 10.

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.

Learning Objectives

- Learn the process of turning an advisory into a working exploit.
- Figure out if a given security patch/hotfix should be applied immediately or not.

- Learn how to read and understand existing exploits.
- Learn to change an existing exploit that failed to work.
- Write reliable exploits and integrate them into Metasploit.
- Learn what shellcode is, how Metasploit shellcode works and how to make shellcode work reliably in your exploit.
- If you have some basic knowledge about win32 exploit development, get a good refresher and learn more advanced topics.
- If you've read the Corelan exploit development tutorials, this class will help you fully understand and master the concepts?
- Expand your reasons to learn how to write exploits for the Win32 platform.
- You will suffer and bleed a bit, learn fast and not intimidated by debuggers and assembly instructions…

Target Audience

Pentesters, auditors, network/system administrators, reverse engineers, malware analysts, developers, members of a security department, security enthusiasts, or anyone interested in exploit development.

Course Outline

- **The x86 environment**
    - System Architecture
    - Windows Memory Management
    - Registers
    - Introduction to Assembly
    - The stack
    - Running 32bit applications on a 64bit OS (wow64)
- **The Exploit Development Lab Environment**
    - Setting up the exploit developer lab
    - Using debuggers and debugger plugins to gather primitives
- **Stack Buffer Overflows**
    - Stack Buffers

- Functions
- Saved return pointer overwrites
- Stack cookies
- Structured Exception Handlers
- etc

- **Egg Hunters**

  - Using Egghunters
  - Egg Hunters in a WoW64 environment

- **Reliability++ & Reusability++**

  - Finding and avoiding bad characters
  - Creative ways to deal with character set limitations

- **Metasploit Framework Exploit Modules**

  - Writing exploits for the Metasploit Framework
  - Porting exploits to the Metasploit Framework

- **ASLR**

  - Bypassing ASLR

- **DEP**

  - Bypassing NX/DEP
  - Return Oriented Programming / Code Reuse (ROP)

During the course, students will get the opportunity to work on real vulnerabilities in real applications and use exploitation techniques that work on default installation of Operating Systems (Windows 10).

REQUIREMENTS

Student Machine/ Laptop Requirements

- A laptop (no netbook) with vmware workstation/virtualbox and enough processing power and RAM (we recommend 4Gb 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 10 (or Windows 7 SP1) no pathes), Kali Linux (fully up-to-date))

Note : you will receive the exact installation instructions after registration, so <u>don't start installling the VMs yet</u>.

All required tools and applications will be provided during the training or will be downloaded from the internet during the training. You must have full administrator access to all machines. You must be able to install and remove software, and you must be able to disable and/or remove firewall/antivirus/… when necessary.

Students Knowledge Pre-Requisites:

Students should

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

No prior knowledge of assembly is required, but it will certainly help if you have some basic knowledge

(In case you're wondering: if you took OSCP/OSCE, and understood the exploitation part of the courses, then you are probably ready for the course)