ZDResearch Training

This is one of our unique courses, because every advanced security research institution has its own tools and methods for exploit development. In this course, we will provide the students with detailed exploit development. This course is divided into two sub-courses, win32 exploitation and browser exploitation. We will provide Linux & OS X exploitation at a later time as well.

ZDResearch

Exploit Development

Course Material

- Interactive Slides
- Video Tutorials
- Downloadable Virtual Machines
- Staff Responding to Every Question

https://training.zdresearch.com/course/exploitdev

ZDResearch Training

https://training.zdresearch.com

Warmup for newbies

- Windows Internals Pre-requirement
- Reversing Basics
- LAB(ImmunityDBG, IDA, SysinternalSuite)

Chapter 1

1.1 Learning it through the Stack
1.2 what is exploitation?
1.3 Stack basics
1.4 Stack overflow bug
1.5 DirectRet Exploitation
1.6 Shellcode
1.7 LAB(CVE-2011-5007)

Chapter 2: Better Stack smashing

2.1 Stack cookie protection
2.2 SEH exploitation
2.3 SafeSEH/SEHOP protections
2.4 SEH protections Bypass
2.5 LAB(CVE-2011-1591)

Chapter 3: Heap of trouble

3.1 Heap basics
3.2 Heap overflow bug
3.3 Write4 Exploitation
3.4 Function Pointer Exploitation
3.5 LAB(CVE-2011-0406)

ZDResearch Training

ZDResearch Training

ZDResearch

Custom Research
Penetration Testing
Advanced training
BA/WA (PoC/Exploits)

ZDResearch

https://training.zdresearch.com