

Assured Exploitation Training

New York City, Jun 8-9

The New York City edition of the two-day Assured Exploitation training will take place in New York on June 8 and 9, 2011. It will be delivered by expert security researchers Dino Dai Zovi and Alex Sotirov.

Registration price

\$2500/student if registered before May 25

\$3000/student if registered on May 25-Jun 8

Early registration is recommended because the class size is limited and may be sold out. Please email ddz@theta44.org to register for the training or if you have any questions. We accept credit cards or purchase orders from approved companies.

Class description

Many security professionals have mastered stack overflows and heap spraying, but these techniques are rarely sufficient when developing modern real-world exploits. Reliable exploitation on Vista and Windows 7 systems requires advanced techniques such as heap layout manipulation, return oriented programming and ASLR information leaks. This course focuses on teaching the principles behind these advanced techniques and will give the students hands-on experience developing real-world exploits.

The course will start off with an in-depth review of the exploitation mitigations introduced in modern operating systems. The instructors will demonstrate their limitations through simple examples and gradually develop the basic exploitation techniques into more complicated methods applicable to real-world exploitation. Unlike most other exploitation courses, we will focus on approaching exploitation as a creative problem-solving process rather than an exercise of applying cookbook techniques to common types of vulnerabilities. Most of the course will focus on the hands-on application of the material through exercises and leading the students through the development of reliable exploits for recently patched vulnerabilities in widely used software. Each student will finish the class with their own personally developed exploit for the Aurora vulnerability in Internet Explorer that evades ASLR and DEP and reliably exploits Windows 7.

Topics

- In-depth review of GS, ASLR, DEP, SafeSEH and SEHOP exploitation mitigations
- Heap implementation details and manipulation of the heap state (including the Windows 7 heap)
- Building primitives for heap layout control in new applications
- Return oriented programming and shellcode development
- Implementing a universal bypass of DEP and ASLR in Internet Explorer 8
- Multistage stack pivots

Prerequisites

Students are expected to be familiar with the basic exploitation techniques for stack and heap overflows on Windows, as described in the Shellcoder's Handbook and similar books. They should be comfortable using assembly level debuggers and have basic familiarity with reverse engineering. The material in this course is designed to be challenging, but we believe that with the help of our expert instructors any dedicated student will be able to master it.

All hands-on exercises in the course will be performed in virtual machines provided by the trainers. You will need a laptop with VMware Workstation or VMware Fusion if using a Mac. The minimum hardware requirements for the laptop are 2GB of memory and a 2.4GHz Core Duo processor.