

- ▼ Zero-day vulnerability discovery, analysis, triage, and exploitation.
- ▼ Advanced exploitation topics, including Windows mitigation bypasses (up to and including Windows 8.1).
- ▼ Several case studies focusing on Internet Explorer, with proprietary exploitation techniques developed by Exodus.
- ▼ Advanced usage of the IDA Pro disassembler.
- ▼ Reverse Engineering using Exodus' award-winning Toolbag IDA Pro plugin.
- ▼ Intermediate to advanced WinDBG usage.

### Prerequisites:

- ▼ Computer with the ability to run a VMWare image (recommended 1GB+ memory)
- ▼ Some familiarity with: IDA Pro, WinDBG, Python, C/C++.
- ▼ x86 ASM fluency.
- ▼ No prior vulnerability discovery experience is necessary.
- ▼ Installed and usable copy of IDA Pro 6.1+, VMware Workstation/Fusion, Python 2.7+.

### Vulnerability Development Master Class

This 5 day course is designed to provide students with a comprehensive and progressive approach to understanding advanced vulnerability and exploitation topics on the Windows platform. Attendees will be immersed in hands-on exercises that impart valuable skills including static and dynamic reverse engineering, zero-day vulnerability discovery, binary instrumentation, and advanced exploitation of widely deployed server and client-side applications.

Taught by the entire Exodus Intelligence team, this course provides students with direct access to our renowned professionals in a setting conducive to individual interactions.

Currently, the course will be offered at three locations in 2015. The venues will be centrally located in their respective cities (details will be provided to registered attendees):

**April 13<sup>th</sup> - 17<sup>th</sup>, 2015**

Austin, TX

\$6,500 USD per student

---

**July 6<sup>th</sup> - 10<sup>th</sup>, 2015**

Amsterdam, The Netherlands

\$6,500 USD per student

---

**September 7<sup>th</sup> - 11<sup>th</sup>, 2015**

Frankfurt, Germany

\$6,500 USD per student

---