

**TRACK:** IT Security Advanced  
**SESSION #:** ITA#4  
**DATE:** Monday April 19, 2010  
**TIME:** 3:45-5:00  
**SESSION TITLE:** "Introduction to Malware Analysis for Security Technologists"  
**SPEAKER(S):** Lenny Zeltser – Security Practice Director/Senior Faculty Member  
**ORGANIZATION:** Savvis/SANS Institute

**ABSTRACT:** "Introduction to Malware Analysis for Security Technologists"

Lenny Zeltser's popular malware analysis course has helped IT administrators, incident responders, and forensics professionals fight malicious code in their organizations. In this practical presentation, he introduces the process of reverse-engineering malicious software. He covers behavioral and code analysis phases, to make this topic accessible even to technologists with a limited exposure to programming concepts. Session participants will learn the fundamentals and associated tools to get started with malware analysis.

The presentation is structured as a walkthrough of examining a trojanized copy of an instant messenger program, to mimic the scenario of a malicious executable having been discovered on a compromised system. Lenny demonstrates several practical approaches to understanding the sample's functionality in a controlled malware analysis laboratory. The session includes both slides and live demos.

Security incident responders benefit from knowing how to reverse-engineer malware, because this process helps in assessing the event's scope, severity, and repercussions. It also assists in containing the incident and in planning recovery steps. Those who perform forensic investigations also benefit from mastering this topic, because they learn how to understand key characteristic of malware present on compromised systems.

**SPEAKER BIO(S):** Lenny Zeltser leads the security consulting practice at Savvis. He is also a board of directors member at SANS Technology Institute, a SANS faculty member, and an incident handler at the Internet Storm Center. Lenny frequently speaks on information security and related business topics at conferences and private events, writes articles, and has co-authored several books.

Lenny is one of the few individuals in the world who have earned the highly-regarded GIAC Security Expert (GSE) designation. He also holds the CISSP certification. Lenny has an MBA degree from MIT Sloan and a computer science degree from the University of Pennsylvania.