

Advanced Malware Analysis

COURSE DESCRIPTION

SecureNinja's (5) five-day immersion course is focused on hands-on malicious code analysis. You'll learn how to perform both dynamic and static analysis of all major file types (PE files, Office Documents, PDF documents, etc). You'll learn how to do a volatile memory analysis (carving malicious executables of RAM), and you'll also learn how to deobfuscate malicious javascript.

WHO WOULD BENEFIT

IT System Administrators, IT Security Professionals

PREREQUISITES

- Students must have administrative rights on a system that meets the following requirements:
 - At least Windows 7
 - At least 4GB of RAM
 - At least 100GB of disk space
 - Running VMWare 9.0
 - NOTE: We can provide properly configured machines for the class if necessary for an additional fee
- Students should be familiar with using Windows and Linux operating environments and be able to troubleshoot general connectivity and setup issues.
- Students should be familiar with VMware Workstation and be able to create and configure virtual machines.
- Students are recommended to have a high-level understanding of key programming concepts, such as variables, loops, and functions; however, no programming experience is necessary.
- Students will be provided with detailed courseware, detailed lab manuals, and copy/paste notes so that even if the student is not very strong technically they will be able to complete the lab exercises and take notes effectively.

COURSE LENGTH

- 5 days

FOLLOW ON COURSES

- Cyber War

COURSE DETAILS

Day 1: Dead Box Forensics

- Recovering Deleted Files
- Dealing with steganography
- Dealing with encryption

Day 2: Dynamic Analysis

- Building an analysis environment
- Identifying Malicious Activity

Day 3: Static Analysis

- Building a malware database archive
- Identifying malicious capability

Day 4: Network Traffic Analysis & Network IDS signature development

- PCAP Analysis
- IDS Signature Development

Day 5: Browser Forensics & Memory Analysis

- Mass Injection Analysis
- Charting malware redirection
- Carving executables out of RAM

ABOUT THE INSTRUCTOR

Joe McCray

Chief Technology Officer and Senior Cybersecurity Instructor

SecureNinja CTO Joe McCray is an Air Force Veteran and has been involved with cybersecurity for over 10 years. Joe has been involved in over 150 very high-level penetration testing assessments and utilizes his “real world hacking accomplishments” to ensure his clients and students obtain effective knowledge transfer.

His extensive experience and deep knowledge, mixed with his comedic style have lead Joe to be one of the most highly sought after speaking experts in the industry. Joe often makes speaking appearances and gives seminars at major events in the security community such as Black Hat, DEFCON, BruCon, Hacker Halted, Hacktivity and more.

Joe is the recipient of the 2009 EC-Council Instructor Circle of Excellence Award and the 2010 EC-Council Instructor of the Year Award. In addition, he is the founder and CEO of Strategic Security, Inc. an IT Security consulting firm that provides in-depth technical security assessments of your network, web application, and regulatory compliance gap analysis