

j8FMbPmLNqq3ghDg0uCsM/Ach5ZVKZETT7gURoaqTGzBZB+T+8d2W53Bke3c7ty
02jjdklhaMFCQHiHQAECwMCAQIZAQAkCRDafWsa0nHzRmAeAJ9yABw8v2fGxaqJ
sKEu29sdXRpb25zIDxpbmZNo9Theories...ofhiLz9E1xTHVQxBBDGknrC1Ng0
0KLB RXF/j5jJQPxXaNUu/It1TQHSiyEumrHNSnn65aUMPnrbV0VJ8hV8N@vsUE1
/kVaWuF1XQDPX0a2ocjPm/No9Cramming...J75nx9AVfPQB8bLQ6mUrfdMZIZt
MDok/76VekyCzsAAgIIANnG7yLuELGDY2m5muBTfjTUcef4gi+ea/nptFB/Q1+X
Y05Ag3qMDoVekyCzk/76sNo1BootnCamps...oDcS7esD0a2ocj6/MDok/76Y05
71q1C8wXo+VMR0U+028W65Szgg2gGnVqMUB9AVfPQB8bLQ6mUrfdMZIZJ+AyDv
XaNUu/It1TQHSi7jb3HZNo2CrashCourses...0KLB RXF/j5jJQPxXaNUu/It1
vaWuF1XQDPX0a2ocj6H0Tt0pW65p1YKTKd/P2NtVfX82j6TaqTCnMMA7AYhSI0N
2GkHrAWG5p1YKTKd/P2NoxCertifications...hQAECwMCAQIZAQAkCRDafWsa
0k3jWApXXB+4VnVnsHitSj8+VMR0U+028W65Szgg2gGnVqMUB/mjsBADJcQqMX0
3q MDok/76Y05AgaoeNoInformation/Dumps...G1rPBvUF7RC4kPVt73hkus
1q1C8wXo+VMR0U+028W65Szgg2gGnVqMUB9AVfPQB8bLQ6mUrfdMZIZJ+AyDvW
h8+Q09 GWG5p1YKTKNo(Web-Based)qLectures...j8FMbPmLNqq3ghDg0uCs
/xm+aYGg9 MDok/76Y05Ag 06Lkwtu+SIfCtz7GTvf/wfEbGMtvzXdsWdAgZ2dS
0a7AYY9VaWuF1XQDPX0a2ocj6H0Tt0pW65p1YKTKd/P2NtVfW5JqcYxX22azNs



Hands-On How-To® Malicious Document Analysis Training

VaWuF1XQDPX0a2ocj6H0Tt0pW65p1YKTKd/P2NtVfX82j6TaqTCnMMA7AYhSI0N
2GkHrAcHowToInstructionsoPrGySbf2cDEq135yWnt9j+/bbf7kc0k3jWAp
/mjsBADfXnmZvQG51NSjJCqHNSnn65aQMReal-WorldSimulationsumrHNSnn
gtypmICQ8mUA7LG3fijK0wKzszmSGZcfsCGbpnqwfXLuh7gSpLQsTmV0U2VjdX
dHkdHands-OnExercisesgU29sdXRpb25zIDxpbmZvQG51dHNLmNvbT6JAFQEE
Uafn/QCjMTQHfQTB8EGBECAAwFAj00sCx ExpertInstructorszVxCAAwFAj+
haMFCQHiHQAECwMCAQIZAQAkCRDafWsa0nHzRmAeAJ9yABw8v2fGxaqJI9/Vftz
02jjdklhaMFCQHiFsxSmallClassSizesIZAQAkCRDafWsa0nHzRmAeAJ9yABw8
q3ghDg0uCsM/ 1xitVjLhd&NMD/XwXV00jHRhs3jMTQHSiyEumrHNSnn65aUMhL
VekyCTailoredCourseszsAAgIIANnG7yLuELGDY2UpdatedContent1FeI70
1XQDPX0a2ocj6H0Tt fFstjvbzySPIxNu 1j9WE5J2CtJ3k2gpXI61Brwv0YAWC
deralbITjAudArsenalofSecurityMTake-AwaysV8N@vEGBEF90G+zVx0Ehs
Aj0uCsM/Ach5ZVKZETT7gURoaqTG8KXipd@gtYwDxfSjxsZ0bybhCXHfV1HHVaJ
CzsumtmAeAJ9yABw8KCRDafWsa0v2f2x1Post-TrainingkSupportlhaMFCQHi
F CQHiHQAECwFQ hAKCRDafW0Sbf2cDEq1VekyCzsAAgIIANnG7yLuELGDY2m5m
QAE35yW2jj SatisfactionGuaranteedlhaMFCQHiHQAECwMCAQIZAQAkCRDa
dklhaMFCQHiHQAECwMCAQIZAQAkCRDafWsa0n0KLB RXF/j5jJQPxXaNUu/It1TQ
HzRmAeAJ9yABw8v2fGxaqJI9/VftzM0KLB RXF/j5jJQPxXaNUu/It1TQHSiyEu

Real-World Scenario:

You have been recruited as the head of information security of a reputable organization, with over 125,000 hosts and 50,000 users. The organization has invested in top-of-the-line perimeter defenses, including firewalls, intrusion detection and prevention systems, virtual private networks (VPNs) and content filtering technologies. The organization also has “well trained” incident responders and intrusion detection analysts who monitor the entries network vigilantly. The employees of this entity are often trained on opening email attachments, even though they may be scanned by the content filtering technologies that you just purchased and deployed.

The perimeter defenses are configured with very simple but stringent rule-sets to prevent cyber adversaries from infiltrating your network. Everything is going well, when on the eve of your long-planned Mediterranean cruise, you receive a call stating that several employees have received some suspicious documents through email and web downloads. You direct the security team to scan the documents for a possible virus, but no virus was detected. Soon the team observes some strange command-and-control communications being initiated from the user systems to an IP address in a foreign country. Unfortunately, the cable news networks are covering the cyber intrusion of your organization and your career is at stake for not preventing this attack in the first place.

Although no anti-virus software was able to detect a malware, your analysts have captured the suspicious document, but lack the knowledge and resources to provide prompt answers to the provocative questions being ask by upper management. Do you have the requisite skills to provide quick and accurate answers pertaining to the above incident and mitigate future attempts?

Cyber attackers now use malicious documents as an attack vector to bypass enterprise perimeter defensive measures and anti-virus solutions. NetSecurity's Hands-On How-To® Malicious Document Analysis course teaches students how to analyze malicious documents such as Microsoft Office and Adobe Acrobat PDF files for the presence of hidden malware. Course participants learn the tools and techniques for reverse-engineering malicious documents, finding and extracting hidden code, Shellcodes, JavaScripts, and VBA macros from an infected document. Students also learn how to disassemble and examine these malicious codes to understand their intent and capabilities. The Hands-On How-To® Lab Exercises (HOHTLEs) covered in the course incorporate significant real-world experience necessary for delivering legally admissible world-class results in the field.

NetSecurity Benefits:

Through years of real-world hands-on cyber security, digital forensics, and incident response experience, NetSecurity has supported Fortune 500 companies and federal agencies such as the IRS, DHS, VA, BBG, DOL, NSF, and DoD. The benefits of our Hands-On How-To® Malicious Document Analysis course include:

- Skills to establish and fortify an organization's security, forensics, and incident response capabilities
- Customized private sessions, tailored towards organizations' unique environments
- Detailed step-by-step and how-to instructions

- Instructor-led and student-performed hands-on exercises
- Real-world simulations of malicious software in a lab environment
- Seasoned expert instructors with real-world hands-on consulting and training experience
- Arsenal of take-aways (tools, templates, guides, and relevant forensics resources)
- Up-to-date course content, addressing emerging malware analysis challenges
- Small class sizes ensuring maximum student-instructor interaction
- Vendor-neutral content, covering commercial and freeware tools

Target Audience:

The Malicious Document Analysis course is targeted towards technical professionals, including:

- Computer Forensics Investigators
- Incident Responders
- Malware Analysts
- Information Security Professionals
- Technology Enthusiasts

Course Format:

- Interactive presentations by security, forensics, and incident response expert instructor
- Hands-On How-To® Lab Exercises performing malicious code analysis

Course Duration: One (1) Day

Course Cost: \$1,295

Course Objectives:

Upon successful completion of the **Hands-On How-To® Malicious Document Analysis** course, each participant will be armed with the knowledge, tools, and processes required to analyze malicious Microsoft Office and Adobe PDF files for the presence of hidden malware. Students learn the tools and techniques for disassembling and reverse-engineering malicious documents, finding and extracting hidden codes, Shellcodes, JavaScripts, and VBA macros from an infected document. Specifically, students will possess relevant knowledge and real-world hands-on skills in:

- Document Structures
- Document Vulnerabilities
- Tools of the Trade
- Malware Extraction
- Malware Analysis

Course Topics:

NetSecurity's Malicious Document Analysis course includes in-depth coverage of real-world scenarios and HOHTLEs in the following areas:

Topics	Discussion and HOHTLEs
Document Structures	<ul style="list-style-type: none">• PDF Document Structures• Microsoft Office Document Structures
Document Vulnerabilities	<ul style="list-style-type: none">• PDF Vulnerabilities• Potentially Dangerous PDF Functions• Office Documents Vulnerabilities
Tools of the Trade	<ul style="list-style-type: none">• OfficeMalScanner• MalHost-Setup• Offvis• PDFiD• PDF-parser• Origami (Walker, PDFscan, Extractjs)• Malzilla• DisView• PDF StructAzer• Many more
Malware Extraction	<ul style="list-style-type: none">• Malware Codes/Specimens (Shellcodes, JavaScripts, and VBA macros)• Locating Malicious Code in a Document• Extracting Malware from PDF Documents• Extracting Malware from Office Documents• Extracting Infected Documents from RAM
Malware Analysis	<ul style="list-style-type: none">• Static Analysis of Malware Specimen• Dynamic Analysis Malware Specimen• Reverse-Engineering & Disassembling Malware

More Information:

For more information about NetSecurity's Hands-On How-To® Training, please contact us at Training@NetSecurity.com or call **1-866-66-HOW-TO (1-866-664-6986)**.