

j8FM6PmLNqq3ghDg0uCsM/Ach5ZVKZETT7gURoaqTGzBZ8+T+8d2W538ke3c7ty  
02jjdk1haMFCQHiHQAECwMCAQIZAQAkCRDafWsa0nHzRmAeAJ9yABw8v2fGxaqJ  
sKEu29sdXRpb25zIDxpmZ**No Theories...**ofhiLz9E1xTHVQxBB0GknrC1NgDr  
0KLbRXF/j5jJQPxXaNUu/It1TQHSiyEumrHNSnn65aUMPnrbV0VJ8hV8N@vsUE1  
/kVaWuF1XQDPX0a2ocjPm**No Cramping...**J75nx9AVfPQB8bLQ6mUrfdMZIZ 9  
MDok/76aVekyCzsAAgIIANnG7yLuELGDY2m5muBTfjTUcef4gi+ea/nptFB/Q1+  
Y05Ag13qMDoVekyCzk/76**No1 Boot Camps...**oDcS7esD0a2ocjb/MDok/76Y05  
71q1C8wXo+VMR0U+028W65Szgg2gGnVqMUB9AVfPQB8bLQ6mUrfdMZIZJ+AyDv  
XaNUu/It1TQHSi7jb3HZ**No2 Crash Courses...**0KLbRXF/j5jJQPxXaNUu/It1  
vaWuF1XQDPX0a2ocjbH0TtOpW65p1YKTkd/P2NtVfX82jbTaqTCnMMa7AYhSI0N  
2GkHrAWG5p1YKTkd/P2 **No Certifications...**hQAECwMCAQIZAQAkCRDafWsa  
0k3jWApXXB+4VnVnsHitSj8+VMR0U+028W65Szgg2gGnVqMUB/mjsBADJCqQMX0  
3q MDok/76Y05Agaoe3**No Information Dumps...**G1rPBvUF7RC4kPVt73hku  
1q1C8wXo+VMR0U+028W65Szgg2gGnVqMUB9AVfPQB8bLQ6mUrfdMZIZJ+AyDvW  
h8+Q9aGwG5p1YKTkg**No (Web-Based) Lectures...**j8FM6PmLNqq3ghDg0uC  
/xm+aYGg9jMDok/76Y05Agr0bLkwtu+SIfCtz7GTvf/wfEbGMtvzXdsWAgZ2dS  
0a7AYY9VaWuF1XQDPX0a2ocjbH0TtOpW65p1YKTkd/P2NtVfW5JqcYxX22azNs



## Hands-On How-To® Malware Analysis Training

VaWuF1XQDPX0a2ocjbH0TtOpW65p1YKTkd/P2NtVfX82jbTaqTCnMMa7AYhSI0N  
2GkHrAc**How-To Instructions**oPrGySbf2cDEq135yWnt9j+/bbf7kc0k3jWAp  
/mjsBADfXnmZvQG51NSjJCqHNSnn65aQM**Real-World Simulations**umrHNSnn  
gtypmICQ8mUA7LG3fijkDwKzszmSGZcfsCGbpnqwfXLuh7gSpLQsTmV0U2VjdXJ  
dHkd**Hands-On Exercises**gU29sdXRpb25zIDxpbmZvQG51dHNLmNvbT6JAFQEE  
Uafn/QCjMTQHfQTB8EGBECAAwFAj00sCx **Expert Instructors**zVxCAAwFAj+  
haMFCQHiHQAECwMCAQIZAQAkCRDafWsa0nHzRmAeAJ9yABw8v2fGxaqJI9/Vftz  
02jjdk1haMFCQHiFsx**Small Class Sizes**IZAQAkCRDfWsa0HzRmAeAJ9yABw8  
q3ghDg0uCsM/ 1xitVjLhd&NMD/XwXV00jHRhs3jMTQHSiyEumrHNSnn65aUMhL  
VekyC**Tailored Courses**zsAAgIIANnG7yLuELGDY2**Updated Content**1FeI70  
1XQDPX0a2ocjbH0Tt fFstjvbzySPIxNu 1j9WE5J2CtJ3k2gpXI61BrwvOYAWC  
deralbITjAud**Arsenal of Security Take-Aways**V8N@vEGBEF90G+zVx0Ehs  
Aj0uCsM/Ach5ZVKZETT7gURoaqTG8KXipd@gtYwdXfSjxsZ0bybhCXHfV1HHVaJ  
CzsumtmAeAJ9yABw8KCRDafWsa0v2f2x1**Post-Training Support**1haMFCQHi  
F CQHiHQAECwFQ hAKCRDafW0Sbf2cDEq1VekyCzsAAgIIANnG7yLuELGDY2m5m  
QAE35yW2jj **Satisfaction Guaranteed**1haMFCQHiHQAECwMCAQIZAQAkCRDa  
dk1haMFCQHiHQAECwMCAQIZAQAkCRDafWsa0n0KLbRXF/j5jJQPxXaNUu/It1TQ  
HzRmAeAJ9yABw8v2fGxaqJI9/VftzM0KLbRXF/j5jJQPxXaNUu/It1TQHSiyEbu

## Real-World Scenario:

You are the leader of an incident response team charged with conducting high-profile cyber crime investigations for a major government agency with 182,522 nodes. This organization is hit with millions of hacking attempts daily. The enterprise network has been under attack for the past two weeks and members of your team have been working around-the-clock to contain the incident. After many man-hours, the network seemed calm and the attack appeared to be thwarted; or so you thought. Exactly one week later, a member of the Tier II team observes that attackers have successfully penetrated valuable systems and are pilfering crucial government data to a foreign country. Some of the malicious software (malware) has been captured, but you have limited expertise to answer critical questions about the compromise. Senior agency's officials are demanding immediate answers as to how the malware got into the network, where it originated from, what critical data was compromised, who created the malware, and how the agency can defend against this type of attack in the future. Do you have the requisite skills to provide quick and accurate answers to the above high profile penetration and mitigate future attempts?

Today's cyber adversaries are highly skilled and sophisticated hackers who are either part of state-sponsored or organized crime. These "elite" hackers are so advanced that current security measures do not detect, let alone prevent their attacks. These criminals are paid and spend ample time conducting reconnaissance about their targets, then customizing their attack towards the victim. The firewall doesn't prevent the attack and the IDS doesn't detect these intrusions. These cyber criminals continue to leverage users' susceptibility to social engineering attacks to infiltrate critical networks. Once inside the network, they lay low on the radar and often go undetected since there are no known signatures.

Malware Analysis is a time-consuming effort that requires specialized expertise, procedures, tools, and real-world analysis skills. NetSecurity's Hands-On How-To® Malware Analysis course teaches students the step-by-step process for quickly analyzing malware to determine the extent of their malicious intent and device appropriate countermeasures. 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® Malware 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 Malware 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 computer forensics and incident response

**Course Duration:** Three (3) Days

**Course Cost:** \$2,995

## Course Objectives:

Upon successful completion of the **Hands-On How-To® Malware Analysis** course, each participant will be armed with the knowledge, tools, and processes required to conduct malware analysis and produce a report that can withstand legal scrutiny. Specifically, students will possess relevant knowledge and real-world hands-on skills in:

- Introduction to Malware Analysis
- Malware Hiding Places
- Building a Malware Analysis Lab (Environment)
- Static Analysis
- Dynamic Analysis
- Code Analysis
- Malicious Document Analysis
- Identifying and Protecting against Malware
- Malware Challenges in the Real-World

## Course Topics:

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

Topics	Discussion and HOHTLEs
<b>Introduction to Malware Analysis</b>	<ul style="list-style-type: none"><li>• Malware Taxonomy</li><li>• Malware Threats</li><li>• Malware Analysis Methodologies</li><li>• Legal Considerations</li><li>• Identifying and Protecting against Malware</li></ul>
<b>Malware Hiding Places</b>	<ul style="list-style-type: none"><li>• Collecting Malware from Live system</li><li>• Identifying Malware in Dead system</li></ul>
<b>Building a Malware Analysis Lab (Environment)</b>	<ul style="list-style-type: none"><li>• Virtual Machine</li><li>• Real Systems</li><li>• Malware Analysis Tools</li></ul>
<b>Static Analysis</b>	<ul style="list-style-type: none"><li>• Detailed File Analysis</li><li>• Database of File Hashes</li><li>• Identifying File Compile Date</li><li>• Identifying Packing/Obfuscation Methods</li><li>• Performing Strings</li><li>• File Signature Analysis</li><li>• Local and Online Malware Scanning</li><li>• Identifying File Dependencies</li></ul>
<b>Dynamic Analysis</b>	<ul style="list-style-type: none"><li>• System Baselineing</li><li>• Host Integrity Monitor</li><li>• Installation Monitor</li><li>• Process Monitor</li><li>• File Monitor</li><li>• Registry Analysis/Monitoring</li><li>• Network Traffic Monitoring/Analysis</li><li>• Port Monitor</li><li>• DNS Monitoring/Resolution</li><li>• Simulating Internet Services</li></ul>
<b>Code Analysis</b>	<ul style="list-style-type: none"><li>• Reverse Engineering Malicious Code</li><li>• Identifying Malware Passwords</li><li>• Bypassing Authentication</li></ul>
<b>Malicious Document Analysis</b>	<ul style="list-style-type: none"><li>• PDF and Microsoft Office Document Structures</li><li>• PDF and Office Documents Vulnerabilities</li><li>• Malware Extraction and Analysis Tools</li><li>• Analysis of Malicious Documents</li></ul>

Topics	Discussion and HOHTLEs
<b>Malware Challenges</b>	<ul style="list-style-type: none"> <li>• Virtual Environment</li> <li>• Live Internet Connection</li> <li>• Real, Fake, and Virtual Services</li> <li>• Anti-Debug and Anti-forensic Malware</li> </ul>

**More Information:**

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