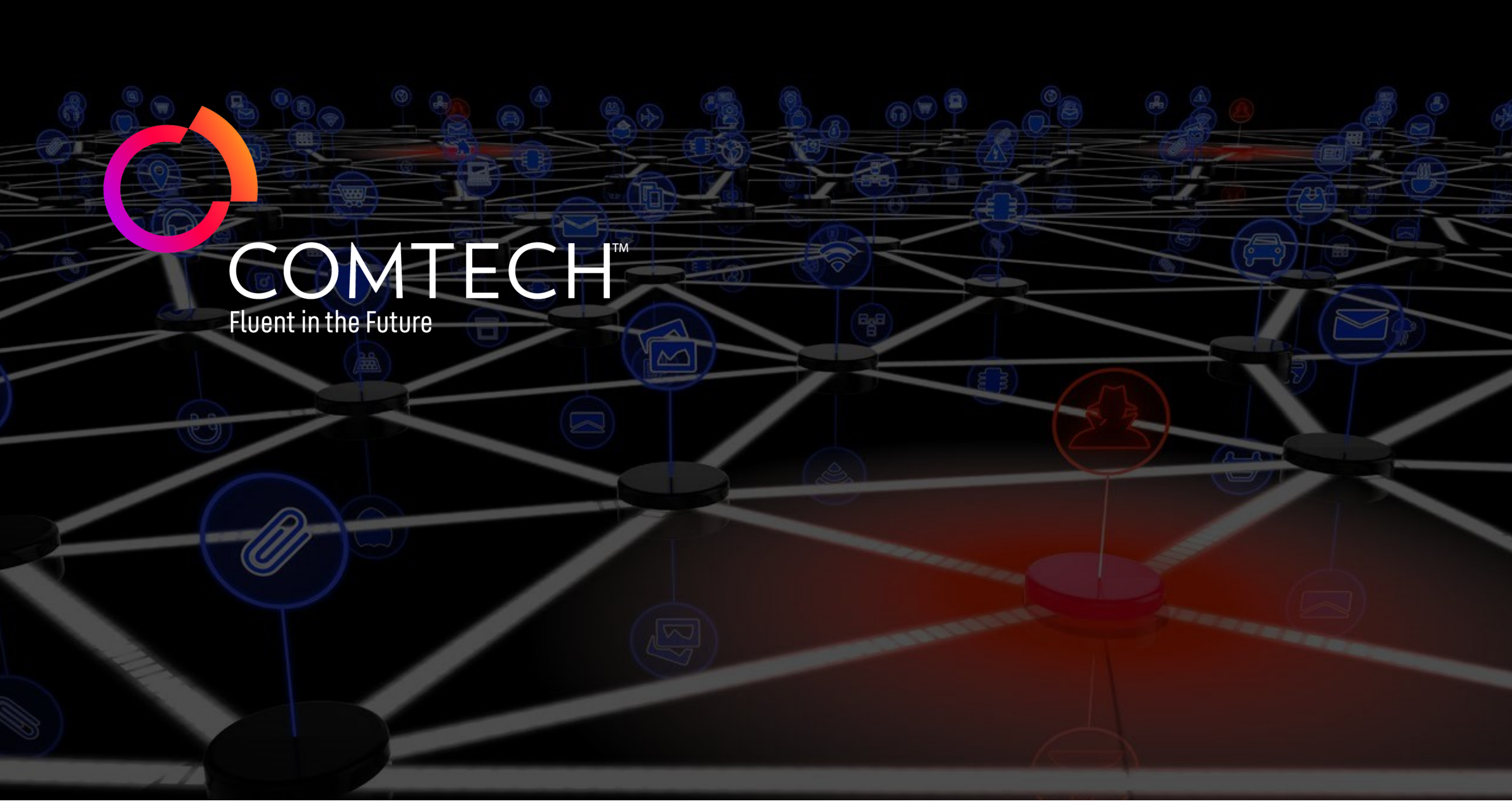

MAL400 Fundamentals of Malware Analysis

Course Overview

MAL400 - Fundamentals of Malware Analysis is an introductory course that exposes students to the theoretical knowledge and hands-on techniques for analyzing malware.

Students will learn how to identify and analyze software that causes harm to users, computers and networks as part of an overall cyber defense and incident response plan. Understanding how malware works and what it was designed to do is crucial to thwarting future attacks.

Objectives

- To obtain the basic skills needed for the identification and analysis of software that causes harm to users, computers and networks

Target Audience

- New malware analysts looking to increase their arsenal of techniques, or others looking to break into the malware analysis field

Estimated Course Length: 24 hours

COMTECH™

comtech.com | cyberstronger.com
275 West Street, Annapolis, MD 21401
© 2023, Comtech Telecommunications Corp. All rights reserved.

Day 1	Day 2	Day 3
Introduction to the overall malware analysis process and methodology. Students define terminology, learn specific malware types and cover fundamental approaches of analysis, in addition to learning how to effectively analyze program code/structure to determine function. Students are challenged with three labs. Day 1 ends with a detailed overview of setting up and using a safe virtual environment for malware analysis.	Day 2 focuses on easy-to-use techniques to dynamically analyze malicious programs by running them in a lab. Students learn to observe true behavior of malware and determine its purpose and functionality via live demos and three challenging specimens they must analyze. Day 2 centers around how malware interacts with the victim's OS by looking at network activity, registry changes and interactions with the file system.	Day 3 closes behavioral analysis and ends with a final fourth lab. Students then begin X86 assembly language. This module is crucial for learning follow-on analysis techniques using debuggers and disassemblers. Students learn key concepts in assembly language to assist follow-on analysis with IDA Pro. IDA Pro is introduced as a disassembler and reverse engineering tool. Considerable time is spent on familiarization with the UI and IDA's numerous features. Plenty of code snippets, demos and two IDA familiarization labs help the student understand both assembly language and how to use IDA Pro.
Topics List ➤ Malware analysis techniques ➤ Identification via antivirus tools and hashing ➤ Analyzing strings, functions, and headers ➤ Use a variety of virtual machines, settings and configurations	**Topics List** ➤ Use of Procmon, Process Explorer and Regshot to understand malicious behavior ➤ Fake network services to aid analysis ➤ Traffic analysis ➤ Network connections ➤ X86 architecture	**Topics List** ➤ Stack vs. Heap ➤ Registers, flags & basic instructions ➤ Conditionals, flow control instructions & jumps ➤ IDA Pro UI intro ➤ Disassembly window (Text vs. Graph Mode) ➤ Jumping to memory addresses

Day 4	Day 5
IDA Pro Introductions continues on Day 4 with the identification and analysis of more complex functions. Students are gradually exposed to more complex malware and its disassembly to build confidence and skills. Students learn techniques needed to identify, categorize and analyze high-level functionality of assembly code. Two labs challenge students to identify a variety of C code constructs in malware specimens as part of an overarching analysis strategy.	Students spend their final day analyzing two malicious programs to further solidify analysis skills focusing on the identification of C code constructs in assembly, and how these high-level constructs correlate to other aspects of the program and its behavior. An instructor-led review of all major topics will be conducted and any final questions will be answered. After the course, students have 90 days to challenge the optional CYBRScore-enabled certification associated with MAL400. The certification presents a malware specimen to the challenger that must be analyzed using the techniques and tools learned in this course. Our behind-the-scenes scoring engine will track progress throughout against a rubric of core skills that must be demonstrated in the hands-on analysis.
Topics List ➤ Cross-references in code ➤ Function identification, analysis & renaming ➤ Imports, exports & structs ➤ Searching through disassembly ➤ Code & data redefinition ➤ Deeper function analysis	

About Comtech

Comtech provides cybersecurity solutions and services tailored to training and workforce development. The CyberStronger product portfolio was created by a team of former National Intelligence Community members who all possess the necessary hands-on, practical cybersecurity experience and abilities required to meet the needs of our demanding customer base. Our experts share the intellectual curiosity to constantly ask the 'why' and 'how' as they develop and deliver truly unique products and services to help close the growing cybersecurity skills gap. The Comtech CyberStronger offerings include off-the-shelf and custom training, hands-on skills labs, and competency-based assessments mapped to cybersecurity job roles.

© 2023, Comtech Telecommunications Corp. All rights reserved.