uCertify

Course Outline

Mastering Malware Analysis

26 Apr 2025

1. Pre-Assessment
2. Exercises, Quizzes, Flashcards & Glossary

   Number of Questions
3. Expert Instructor-Led Training
4. ADA Compliant & JAWS Compatible Platform
5. State of the Art Educator Tools
6. Award Winning Learning Platform (LMS)
7. Chapter & Lessons

   Syllabus

   Chapter 1: Preface

   Chapter 2: Cybercrime, APT Attacks, and Research Strategies

   Chapter 3: A Crash Course in Assembly and Programming Basics

   Chapter 4: Basic Static and Dynamic Analysis for x86/x64

   Chapter 5: Unpacking, Decryption, and Deobfuscation

   Chapter 6: Inspecting Process Injection and API Hooking

   Chapter 7: Bypassing Anti-Reverse Engineering Techniques

   Chapter 8: Understanding Kernel-Mode Rootkits

   Chapter 9: Handling Exploits and Shellcode

   Chapter 10: Reversing Bytecode Languages – .NET, Java, and More

   Chapter 11: Scripts and Macros – Reversing, Deobfuscation, and Debugging

   Chapter 12: Dissecting Linux and IoT Malware

   Chapter 13: Introduction to macOS and iOS Threats

   Chapter 14: Analyzing Android Malware Samples

   Videos and How To
8. Practice Test

   Here's what you get

   Features
9. Live labs

Lab Tasks

Here's what you get

1. Pre-Assessment

Pre-Assessment lets you identify the areas for improvement before you start your prep. It determines what students know about a topic before it is taught and identifies areas for improvement with question assessment before beginning the course.

2. Exercises

There is no limit to the number of times learners can attempt these. Exercises come with detailed remediation, which ensures that learners are confident on the topic before proceeding.

3. Quiz

Quizzes test your knowledge on the topics of the exam when you go through the course material. There is no limit to the number of times you can attempt it.

4. flashcards

Flashcards are effective memory-aiding tools that help you learn complex topics easily. The flashcard will help you in memorizing definitions, terminologies, key concepts, and more. There is no limit to the number of times learners can attempt these. Flashcards help master the key concepts.

5. Glossary of terms

uCertify provides detailed explanations of concepts relevant to the course through Glossary. It contains a list of frequently used terminologies along with its detailed explanation. Glossary defines the key terms.

6. Expert Instructor-Led Training

uCertify uses the content from the finest publishers and only the IT industry's finest instructors. They have a minimum of 15 years real-world experience and are subject matter experts in their fields. Unlike a live class, you can study at your own pace. This creates a personal learning experience and gives you all the benefit of hands-on training with the flexibility of doing it around your schedule 24/7.

7. ADA Compliant & JAWS Compatible Platform

uCertify course and labs are ADA (Americans with Disability Act) compliant. It is now more accessible to students with features such as:

- Change the font, size, and color of the content of the course
- Text-to-speech, reads the text into spoken words
- Interactive videos, how-tos videos come with transcripts and voice-over
- Interactive transcripts, each word is clickable. Students can clip a specific part of the video by clicking on a word or a portion of the text.

JAWS (Job Access with Speech) is a computer screen reader program for Microsoft Windows that reads the screen either with a text-to-speech output or by a Refreshable Braille display. Student can easily navigate uCertify course using JAWS shortcut keys.

8. State of the Art Educator Tools

uCertify knows the importance of instructors and provide tools to help them do their job effectively. Instructors are able to clone and customize course. Do ability grouping. Create sections. Design grade scale and grade formula. Create and schedule assessments. Educators can also move a student from self-paced to mentor-guided to instructor-led mode in three clicks.

9. Award Winning Learning Platform (LMS)

uCertify has developed an award winning, highly interactive yet simple to use platform. The SIIA CODiE Awards is the only peer-reviewed program to showcase business and education technology's finest products and services. Since 1986, thousands of products, services and solutions have been recognized for achieving excellence. uCertify has won CODiE awards consecutively for last 7 years:

- **2014**
    1. Best Postsecondary Learning Solution

- **2015**
    1. Best Education Solution

2. Best Virtual Learning Solution
3. Best Student Assessment Solution
4. Best Postsecondary Learning Solution
5. Best Career and Workforce Readiness Solution
6. Best Instructional Solution in Other Curriculum Areas
7. Best Corporate Learning/Workforce Development Solution

- **2016**
    1. Best Virtual Learning Solution
    2. Best Education Cloud-based Solution
    3. Best College and Career Readiness Solution
    4. Best Corporate / Workforce Learning Solution
    5. Best Postsecondary Learning Content Solution
    6. Best Postsecondary LMS or Learning Platform
    7. Best Learning Relationship Management Solution

- **2017**
    1. Best Overall Education Solution
    2. Best Student Assessment Solution
    3. Best Corporate/Workforce Learning Solution
    4. Best Higher Education LMS or Learning Platform

- **2018**
    1. Best Higher Education LMS or Learning Platform
    2. Best Instructional Solution in Other Curriculum Areas
    3. Best Learning Relationship Management Solution

- **2019**
    1. Best Virtual Learning Solution
    2. Best Content Authoring Development or Curation Solution
    3. Best Higher Education Learning Management Solution (LMS)

- **2020**

1. Best College and Career Readiness Solution
2. Best Cross-Curricular Solution
3. Best Virtual Learning Solution

10. Chapter & Lessons

uCertify brings these textbooks to life. It is full of interactive activities that keeps the learner engaged. uCertify brings all available learning resources for a topic in one place so that the learner can efficiently learn without going to multiple places. Challenge questions are also embedded in the chapters so learners can attempt those while they are learning about that particular topic. This helps them grasp the concepts better because they can go over it again right away which improves learning.

Learners can do Flashcards, Exercises, Quizzes and Labs related to each chapter. At the end of every lesson, uCertify courses guide the learners on the path they should follow.

Syllabus

Chapter 1: Preface

- Who this course is for
- What this course covers
- To get the most out of this course
- Conventions used

Chapter 2: Cybercrime, APT Attacks, and Research Strategies

- Why malware analysis?
- Exploring types of malware

- The MITRE ATT&CK framework explained
- APT and zero-day attacks and fileless malware
- Choosing your analysis strategy
- Setting up the environment
- Summary

Chapter 3: A Crash Course in Assembly and Programming Basics

- Basics of informatics
- Architectures and their assembly
- Becoming familiar with x86 (IA-32 and x64)
- Exploring ARM assembly
- Basics of MIPS
- Diving deep into PowerPC
- Covering the SuperH assembly
- Working with SPARC
- Moving from assembly to high-level programming languages
- Summary

Chapter 4: Basic Static and Dynamic Analysis for x86/x64

- Working with the PE header structure
- Static and dynamic linking
- Using PE header information for static analysis
- PE loading and process creation
- Basics of dynamic analysis using OllyDbg and x64dbg
- Debugging malicious services
- Essentials of behavioral analysis
- Summary

Chapter 5: Unpacking, Decryption, and Deobfuscation

- Exploring packers
- Identifying a packed sample
- Automatically unpacking packed samples
- Manual unpacking techniques
- Dumping the unpacked sample and fixing the import table
- Identifying simple encryption algorithms and functions
- Advanced symmetric and asymmetric encryption algorithms
- Applications of encryption in modern malware – Vawtrak banking Trojan

- Using IDA for decryption and unpacking
- Summary

Chapter 6: Inspecting Process Injection and API Hooking

- Understanding process injection
- DLL injection
- Diving deeper into process injection
- A dynamic analysis of code injection
- Memory forensics techniques for process injection
- Understanding API hooking
- Exploring IAT hooking
- Summary

Chapter 7: Bypassing Anti-Reverse Engineering Techniques

- Exploring debugger detection
- Handling the evasion of debugger breakpoints
- Escaping the debugger
- Understanding obfuscation and anti-disassemblers

- Detecting and evading behavioral analysis tools
- Detecting sandboxes and VMs
- Summary

Chapter 8: Understanding Kernel-Mode Rootkits

- Kernel mode versus user mode
- Windows internals
- Rootkits and device drivers
- Hooking mechanisms
- DKOM
- Process injection in kernel mode
- KPP in x64 systems (PatchGuard)
- Static and dynamic analysis in kernel mode
- Summary

Chapter 9: Handling Exploits and Shellcode

- Getting familiar with vulnerabilities and exploits
- Cracking the shellcode
- Exploring bypasses for exploit mitigation technologies

- Analyzing Microsoft Office exploits
- Studying malicious PDFs
- Summary

Chapter 10: Reversing Bytecode Languages – .NET, Java, and More

- The basic theory of bytecode languages
- .NET explained
- .NET malware analysis
- The essentials of Visual Basic
- Dissecting Visual Basic samples
- The internals of Java samples
- Analyzing compiled Python threats
- Summary

Chapter 11: Scripts and Macros – Reversing, Deobfuscation, and Debugging

- Classic shell script languages
- VBScript explained
- VBA and Excel 4.0 (XLM) macros and more

- The power of PowerShell
- Handling JavaScript
- Behind C&C – even malware has its own backend
- Other script languages
- Summary

Chapter 12: Dissecting Linux and IoT Malware

- Explaining ELF files
- Exploring common behavioral patterns
- Static and dynamic analysis of x86 (32- and 64-bit) samples
- Learning about Mirai, its clones, and more
- Static and dynamic analysis of RISC samples
- Handling other architectures
- Summary

Chapter 13: Introduction to macOS and iOS Threats

- Understanding the role of the security model
- File formats and APIs
- Attack stages

- Advanced techniques
- Static and dynamic analysis of macOS and iOS samples
- The analysis workflow
- Summary

Chapter 14: Analyzing Android Malware Samples

- (Ab)using the Android internals
- Understanding Dalvik and ART
- File formats and APIs
- Malware behavior patterns
- Static and dynamic analysis of threats
- Summary

11. Practice Test

Here's what you get

Features

Each question comes with detailed remediation explaining not only why an answer option is correct but also why it is incorrect.

Unlimited Practice

Each test can be taken unlimited number of times until the learner feels they are prepared. Learner can review the test and read detailed remediation. Detailed test history is also available.

Each test set comes with learn, test and review modes. In learn mode, learners will attempt a question and will get immediate feedback and complete remediation as they move on to the next question. In test mode, learners can take a timed test simulating the actual exam conditions. In review mode, learners can read through one item at a time without attempting it.

12.  Live Labs

The benefits of live-labs are:

- Exam based practical tasks
- Real equipment, absolutely no simulations
- Access to the latest industry technologies
- Available anytime, anywhere on any device
- Break and Reset functionality
- No hardware costs

Lab Tasks

Cybercrime, APT Attacks, and Research Strategies

- Scanning and Classifying Different Types of Viruses
- Using the Backdoor Tool
- Examining Spyware

- Simulating a DDoS Attack
- Examining MITRE ATT&CK
- Performing Reconnaissance
- Installing VirtualBox

A Crash Course in Assembly and Programming Basics

- Performing the AND Operation
- Understanding the Circular shift (Rotate) Operator
- Understanding OR and XOR Operators

Basic Static and Dynamic Analysis for x86/x64

- Displaying the PE Header
- Analyzing a Sample Using OllyDbg
- Using Resource Monitor
- Tracing Packets Using Wireshark

Unpacking, Decryption, and Deobfuscation

- Turning on DEP
- Using an Asymmetric Algorithm
- Using a Symmetric Algorithm

Inspecting Process Injection and API Hooking

- Exploring Windows Registry Entries
- Performing Code Injection
- Using Volatility for Memory Forensic Analysis

Bypassing Anti-Reverse Engineering Techniques

- Detecting Virtualization through Registry Keys

Understanding Kernel-Mode Rootkits

- Detecting Rootkits
- Performing an MITM Attack

Handling Exploits and Shellcode

- Launching a DoS Attack
- Performing Local Privilege Escalation

Reversing Bytecode Languages – .NET, Java, and More

- Exploring Packers Using the PEiD Tool

Scripts and Macros – Reversing, Deobfuscation, and Debugging

- Executing Batch Scripting Commands in Windows
- Understanding the Bash Command-line Interface
- Executing PowerShell Command-line Arguments

Dissecting Linux and IoT Malware

- Using Syscalls for Filesystem, Network, and Process Management
- Accessing the Assembly Code
- Using TCPdump to Capture Packets

Analyzing Android Malware Samples

- Running the Android Emulator on a Virtual Machine

Here's what you get

33	30	01:03
LIVE LABS	VIDEO TUTORIALS	HOURS