Malware Analyst Professional - Level 1

About TrainSec Academy

TrainSec Academy is an online learning hub for current and aspiring cybersecurity pros who understand the need for excellence. Level up or change career using skill-expanding modular learning way. We turn beginners into experts and experts into masters. TrainSec Academy is designed for those who are serious about being at the vanguard of the latest knowledge, skills and trends. We're already working with the best.

Course Overview

In this malware analysis and reverse engineering course, you will delve into the inner core of dissecting different malware types and variants, understand the adversarial mindset behind them and the used TTPs. At the end of the course, you will gain the power and knowledge to win any malware coming your way.

Course Objectives

This course lays the groundwork for mastering malware analysis. Gain essential skills, earn certification, and launch your cybersecurity career with confidence!

Course Format

- **URL**: https://trainsec.net/courses/malware-analyst-professional-level-1/
- **Scope and Mode**: 56 Learning materials, spanning on around 8.5 hours of online videos and presentations.
- **Format**: Pre-recorded Videos and Presentations, discussion group and personal trainer support.
- **Pace**: Self-paced
- **Platform**: TrainSec.net Learning Platform, Discord server.

Course Content

Introduction and Lab Setup

- What is Malware and what common types of Malware
- What is Malware Analysis and its purposes
- Types and levels of Malware Analysis (static, dynamic, and code reverse engineering)

- Setting up the Lab (lab architecture overview, setting up Windows Malware analysis lab).
- Optimizing the lab for better and more efficient Malware Analysis
- Deploying Flare-VM
- Deploying REmnux and connecting to InetSim
- Tools of the trade (deployment and overview)

Content:

1. Malware Analysis Lab OVA Deployment
2. Introduction to Malware Analysis • 11 mins
3. Lab Setup - Intro • 3 mins
4. Lab Setup - Deploying Flare-VM • 5 mins
5. Lab Setup - Connecting to INetSim • 13 mins

Introduction to Code Reverse Engineering

- The four stages of software development
- Basic C programming examples
- Deploying Visual Studio and compilation tools
- Analyzing compiled assembly code with IDA

Content:

1. Installing Visual Studio • 4 mins
2. The four stages of Development • 5 mins
3. Basic C Code Example - Part 1 • 7 mins
4. Basic C Code Example - Part 2 • 11 mins
5. example1.c
6. example2.c
7. Basic Reverse Engineering - Part 1 • 25 mins
8. Basic Reverse Engineering - Part 2 • 5 mins

The PE Structure

1. PE Structure Overview - Part 1 • 13 mins
2. PE Structure Overview - Part 2 • 14 mins
3. PE-exe vs. PE-dll • 8 mins

Static Malware Analysis

- Identifying common file formats using hex editors and PE parsers
- Malware fingerprinting using calculated hashes
- Using VirusTotal for threat intelligence and multi-AV scanning purposes
- File string extraction and decoding

- Determining obfuscation and Packers
- Inspecting PE header for valuable information and IoC (Indicators of Compromise) gathering
- Classifying malware families and variants
- Packing detection and analysis
- Optimal reverse engineering approaches and methodologies
- Leveraging IDA's Pseudo Decompilation feature
- Approaching and reading function documentation
- Renaming functions/subroutines
- Saving IDA's Reverse Engineering Progress
- Writing your own custom YARA signatures
- Static Reverse Engineering with IDA Pro
- Breaking the FlawedAmmyy RAT into pieces

Content:

1. Purpose and Goals of Malware Analysis • 5 mins
2. Understanding Signature Names and VirusTotal Overview • 12 mins
3. IoC vs. IoA • 8 mins
4. Identifying File Types • 5 mins
5. Calculating Hashes • 11 mins
6. Strings Extraction • 6 mins
7. Packing Analysis - Part 1 • 9 mins
8. Packing Analysis - Part 2 • 15 mins
9. Packing Analysis - Part 3 • 4 mins
10. Identifying Malicious Functionality • 10 mins
11. Approaching and Reading Documentations • 10 mins
12. Dissecting FlawedAmmyy - Part 1 • 26 mins
13. Dissecting FlawedAmmyy - Part 2 • 26 mins
14. Saving your RE progress to an IDB File • 2 mins

Dynamic Malware Analysis

- Logging system events using Procmon
- Sniffing and analysis of network traffic using Wireshark
- Execution and analysis of DLL files using Rundll32.exe
- Monitoring Windows API functions using API Logger
- Inspecting process command line arguments using CMD Watcher
- Dynamic Reverse Engineering (debugging) with IDA Pro
- FlawedAmmyy RAT attack flow analysis
- Unpacking/decrypting FlawdAmmyy RAT in-memory runtime payload
- Writing a YARA rule to detect and hunt FlawedAmmyy variants

Content:

1. Introduction to Dynamic Analysis • 29 mins
2. Working with Process Explorer • 10 mins
3. Extracting IoCs using Process Hacker • 6 mins
4. Working with Procmon • 11 mins
5. Monitoring WinAPI Functions using API Logger • 3 mins
6. Inspecting Process Command Line Parameters using CMD Watcher • 7 mins
7. Debugging DLL Files with IDA Disassembler • 5 mins
8. FlawedAmmyy RAT - Attack Flow PCAP Analysis Overview • 16 mins
9. FlawedAmmyy RAT Dynamic Analysis • 23 mins
10. FlawedAmmyy RAT Dynamic Reverse Engineering - Part 1 • 28 mins
11. FlawedAmmyy RAT Dynamic Reverse Engineering - Part 2 • 27 mins
12. Detecting FlawedAmmyy RAT with YARA • 25 mins

Malicious Documents Analysis

- Analyzing VBA Macros inside Office documents
- Analyzing a VBA Macros shellcode process injection
- Analyzing PDF exploits leveraging JavaScript

Content:

1. Introduction to Malicious Documents • 8 mins
2. Introduction to Analyzing Malicious PDF Files • 3 mins
3. Analyzing the CVE-2008-2992 PDF Exploit • 6 mins
4. Analyzing VBA Macros - Introduction • 6 mins
5. Analyzing VBA Macros - Shellcode Injection • 15 mins

Malware Lab Samples

- 404 Not Found - Isn't that a Mystery?!
- spaceFlawedAmmyy.zip
- Malicious Documents Lab Samples.zip

YARA Rules Examples

- sodinokibi.yara
- PE.yara
- WannaCry.yara
- UPX.yara
- Cryak.yara

Required Materials

- **Prerequisites**:
  - Basic understanding of networking: TCP/IP, Routing, Forwarding
  - Reading and understanding code
  - Basic understanding of Windows Server and Linux Shell commands
  - Basic understanding of well-known protocols such as HTTP/HTTPS, DNS, SMTP, FTP, SSH
  - PC/MAC with Intel i5/i7/i9 CPU, 16GB of RAM and an SSD storage
  - VMware Workstation/Fusion installed
- **Additional Resources**: https://discord.com/invite/qugcNyWdaU

Instructor Information

- **Name**: Uriel Kosayev
- **Email**: uriel@TrainSec.net
- **Trainers Biography**:
  Uriel: Security researcher, consultant, and the author of the "*Antivirus Bypass Techniques book"* who lives both on the offensive and defensive fronts. Passionate about malware research, and red teaming while providing real-world security solutions.

Contact & Support

For any course-related or billing-related inquiries, please contact info@TrainSec.net