ZDResearch Training

ZDResearch

Reverse Engineering

Reverse engineering is the art of understanding machine code and meddling with it. An expert reverse engineer can change a binary (compiled) application in any way s/he wants, just like s/he has the source code. This course teaches you to be an expert reverse engineer. On top of that, you will learn methods to increase your performance, you will get to know the tools of the trade and master them, learn how to protect against reverse engineering and more importantly, how to bypass all those protections. Feel free to check the brief course syllabus, and contact us if you need a more detailed outline.

Course Material

- ❖ Interactive Slides
- ❖ Video Tutorials
- ❖ Downloadable Virtual Machines
- ❖ Staff Responding to Every Question

https://training.zdresearch.com/course/re

ZDResearch Training

https://training.zdresearch.com

1. Reverse Engineering Essentials

1.1. x86 Assembly Language

1.2. OS Internals and API

1.3. PE Tour

1.4. Reversing Tools

1.4.1. Debuggers

1.4.2. Disassemblers and Hex Editors

1.4.3. Memory Dumpers/PE Editors

1.4.4. Monitoring Tools

1.4.5. Unpacking Tools

1.5. Hands-On-Lab

2. Legal Software Protection Reversing

2.1. Necessary Tools To Start Cracking (IDA Pro / OllyDbg)

2.1.1. Basic Features of IDA Pro

2.1.2. Basic Features of OllyDbg

2.2. Useful APIs In Reversing

2.2.1. APIs For Different Compilers

2.2.2. Breakpoints, Fixed vs Conditional

2.3. How To Use Your Tools Practically

2.3.1. Attacking a Password Protected Target

2.3.2. Attacking a Serial Number Protected Target

2.4. Byte Patching, EXE vs DLL

2.4.1. Using Hex Editors vs IDA Pro / OllyDbg

3.5. Patching Techniques for Packed / Protected Targets

3.5.1. Writing Loaders

3.5.2. Inline Patching

3.5.3. Hooking and DLL Injection

3.6. Hands-On-Lab

4. Dealing With non-executable files

4.1. Introduction To non-execute files

4.1.1. Analyzing Document files (PDF , DOC , SWF , ETC)

4.1.2. Dealing with Java Class Files

4.1.3. Dealing with Java Jar Files

4.1.4. Dealing with .NET assemblies

4.1.5. Dealing with JavaScript

4.1.6. Analyzing Shellcodes

4.1.7. Hands-On-Lab

5. Malware Reverse Engineering

5.1. Introduction to Malware

5.2. Malware Classification

5.3. Isolating Malwares

5.4. Applying What You Learned On Malwares

5.5. Static Analysis of Malwares With IDA Pro

ZDResearch Training

ZDResearch

ZDResearch

Custom Research

Penetration Testing

Advanced training

BA/WA (PoC/Exploits)

https://training.zdresearch.com