x86 Disassembly and Advanced Static Malware Analysis

WORKSHOP OVERVIEW

This professional deep technical workshop offers a systematical foundation for low-level security software reverse-engineering intel architecture x86 and software analysts, taught from an offensive security research perspective. This class helps you bootstrap into the areas of reverse engineering, vulnerability exploitation, operating system design, code optimization, and compiler design. Key objectives: Software, Intel Architecture, Reverse-Engineering, and Analysts.

Once you've taken this class, it will open the door to all the other specialty areas that depend on assembly knowledge. Although Intel® 64 and IA-32 Architectures Software Developer's Manual have 5060 pages+, students will develop the ability to understand the core concepts behind most programs by learning common programming instructions and their variations.

This workshop expose students to all the essential theory required to analyze software for defensive and offensive, respectively. as well as fundamental practical skills. 40% of the time will be spent bootstrapping knowledge of fully OS-independent aspects of Intel architecture. 60% will be spent learning Reverse-Engineering and analysis of malicious programs.

All labs in this workshop are based on real life tasks.

AUDIENCE

- UiTM Cyberheroes Club Members
- Professional security researchers, malware reverse engineering and reverse engineers.
- People interested in reverse engineering, malware analysis, vulnerability research, exploits, and mitigations.
- Developers who want to understand the correspondence between high level code and machine code.
- People who want to better understand the low level hardware mechanisms which support binary program execution and operating system design.

PREREQUISITES

Essential:

- Must have familiarity with basic programming.
- Assembly/C/C++ (reading level);
- Linux command line and build environment.

Recommended:

- x86/x86_64 assembly language;
- some experience with software analysts.
- basic OS and hardware design concepts.

Hardware:

Students should bring a laptop capable of running a 64 bit version of Windows as specified below, with at least 8GB of RAM, so it can comfortably run multiple virtual machines.

ABOUT THE INSTRUCTOR

Fatah Hashim is a software security researcher specializing in offensive and defensive security research, analysis, and development. His professional career involves low-level programming, reverse engineering, antivirus operation, evasion, malware, vulnerability, and windows internals. His recent work includes research about antivirus research engine bypass: static/dynamic evasion.

Having devoted most of his life to the researching of software security, Throughout his teen years he alternated learning between different programming languages, C, C++, Assembly, Powershell, VB, and Python. His ultimate goal is to understand how computers work from the highest of high levels to the lowest of low levels.

LEARNING OBJECTIVES

Upon completion of this workshop class the students are expected to have obtained the following knowledge and skills:

- Ability to understand the core set of Intel x86 architecture and assembly so as to be able to read and understand short programs in disassembled form.
- Live demo lecture style. Step-by-step instructions for all the hands-on lab exercises performed in the workshop to facilitate the learning experience.
- Knowledge of the classes, techniques for analyzing binary programs with disassemblers. As well as providing a deeper understanding of how disassemblers actually work.
- Provide detailed knowledge on analysis methodology, tools and techniques.
- Ability to analyze code and behavior, identify and characterize functionalities of malicious software, particularly focusing on self-defense mechanisms in Windows executables.
- Perform basic and advanced static analyses of malware and unknown binary files

WORKSHOP OUTLINE

- How to set up a safe sandbox environment and utilise binary analysis tools, particularly on Windows malware and binary files
- Introduction to Code Reverse Engineering
- x86 disassembly
- Overview of malware and possible analysis techniques
- Understanding Signature Names
- IOA vs IOC
- Identifying Malicious Functionality
- Windows API
- Using Interactive Disassembler Professional (IDA Pro)
- Dissecting Malicious Software
- Anti Reverse Engineering

RESERVED FOR NOTES

CHANGE LOG

20.06.2024 Workshop Outline Updated
18.06.2024 Syllabus Updated
12.06.2024 Syllabus Under Review For Update
10.06.2024. Audience Updated
10.06.2024. Syllabus Published.