Module C3: static analysis for binary sre - Disassemblers and Decompilers.

**Module Description:** This module will focus on the use of disassemblers (e.g., *IDA Pro*, *Hopper*, *BeaEngine*, and online disassemblers), and decompilers (e.g., *Hopper* and online decompilers), to include their capabilities and limitations. While *IDA Pro* is the premier tool in this space, it is expensive, so materials will target the use of functionality found in the freeware/demo version of IDA to ensure that it can be widely utilized. Functionality in other decompilers (many of which are far more affordable the *IDA Pro*) will also be covered, but the primary focus will be the common capabilities and limitations of such tools, regardless of the specific tool that is available to the instructor or student. Decompilers will be covered but with less emphasis (as they are often extremely expensive, and also tend to be less extensively used as a student becomes comfortable with disassemblers, particularly in the malware analysis space).

**Prerequisite Knowledge:** This is intended to be a follow-up to Module C2: Basic static analysis tools.

**Length of Completion**: Module – More than 4 and less than 10 hours

**Level of Instruction:** This module intended to be an undergraduate or graduate course for technical majors.

**Learning Setting:** This module is intended for in-class.

**Lab Environment:** VMs and containers that include the exercises and challenge materials to ensure consistency and ease of deployment.

**Activity/Lab Tasks:** A series of hands-on exercises with associated materials to guide instructors and/or students through the process

* Hands-on exercises and challengesduring this module will include the static analysis of various binaries of increasing complexity using disassemblers, including some malware samples, and an exercise in which students create, exchange, examine, and present their analysis of new binaries within the class.

**Lab Files Needed:** All files are contained in the VMs.

# learning outcomes

MODULE learning oUTCOMES

Upon successful completion of this module, the student should be able to:

* Analyze and explain how decompilers and disassembler work,
* Use a disassembler (such as IDA Pro) to perform static reverse engineering of binary samples.
* Use a decompiler (such as that found in Hopper) to perform static reverse engineering of binary samples.
* Identify and navigate decompiler and disassembler functionality.

# module Details

**Interconnection:** This module is part of a 15-week Software Reverse Engineering (SRE) Course. The 15 modules are:

* Module A1: x86 and x64 architectures and assembly languages
* Module A2: ARM architectures and assembly languages
* Module A3: "Forward Engineering"
* Module B1: Approaches
* Module C1: Techniques for the safe handling of files of unknown origin and /or functionality
* Module C2: Basic static analysis tools.
* **Module C3: Disassemblers and Decompilers**
* Module D1: Sandboxing and other techniques for the safe execution/opening of files of unknown origin and /or functionality.
* Module D2: Basic dynamic analysis tools.
* Module D3: Debuggers
* Module D4: Network Traffic Analysis
* Module D5: Patching binaries
* Module E1: Obfuscation and Anti-SRE
* Module F1: Non-Binary SRE

**Instructional Files and Online Resources that are Needed:**

PowerPoint file: SRE-C3-Lecture.pptx

Lab Environment: SRELNX-2.ova

Lab Narrative: SRE-C3-Lab.docx

Supplementary Reading:

Sikorski, M. & Honig, A. (2012). *Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software.* San Francisco:No Starch Press.

Eagle, C. (2011). *The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler (2nd ed.).* San Francisco:No Starch Press.

**Assessment:**

The learning objectives are assessed through the following methods:

1. ASKs: There are questions in the note sections for the instructor to involve the students in the lesson and assess their grasp of the concepts.
2. LABs: There are lab exercises associated with this lesson

# Lessons

**Warm Up:** See SRE-C3-Lecture.pptx

**Lesson:** See SRE-C3-Lecture.pptx

**Active Learning Activity:** See SRE-C3-Lab.docx