Module d1: Sandboxing and other techniques for the safe execution/opening of files of unknown origin and/or functionality.

**Module Description:** Execution of binaries or opening other files of unknown origin and/or functionality, is generally recognized to be potentially dangerous (as opposed to simply storing or transmitting them, as discussed in module C1, where the risk exists but is generally not recognized). This module address techniques by which we can safely execute binaries and open files through sandboxing techniques (including network limitations or even air gapping hosts, virtualization, and reimaging hosts, etc.).

**Prerequisite Knowledge:** This is intended to be a follow-up to Module C3: Disassemblers and Decompilers

**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:** The objective of this lab is to demonstrate mastery of the module learning outcomes by instrumenting a sandbox and understanding and minimizing the potential effects of the instruments on the sandbox.

**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:

* Instrument a sandbox.
* Configure sandbox tools to observe the behavior of malware.
* Identify and measure the potential effects of the instruments on the environment.
* Take steps to minimize the impact of the instruments on the environment.

# 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 Needed:**

PowerPoint file: SRE-D1-Lecture.pptx

Lab Environment: SRELNX-2.ova (Format may vary)

Lab Narrative: SRE-D1-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-D1-Lecture.pptx

**Lesson:** See SRE-D1-Lecture.pptx

**Active Learning Activity:** See SRE-D1-Lab.docx