Module d2: Dynamic analysis for binary sre - Basic dynamic analysis tools.

**Module Description:** This module will include coverage of tools such as *strace*, *ltrace*, various *sysinternals* tools, *ld\_preload*, etc., to determine various characteristics of binary samples. While more advanced tools (such as debuggers) are often used for dynamic analysis, much can often be learned from these more basic tools, and as such it is important to understand their capabilities, limitations, and risks.

**Prerequisite Knowledge:** This is intended to be a follow-up to Module D1: Sandboxing and other techniques for the safe execution/opening of files of unknown origin and /or functionality.

**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 dynamic analysis of various binaries of increasing complexity using basic tools

**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 mitigate the risk associated with dynamic analysis of malware.
* Design and execute dynamic analysis of a file using appropriate tools and techniques.
* Replicate services such as networks, traffic, users, etc. to enable dynamic analysis of malware samples.
* Evaluate and apply appropriate dynamic analysis tools and techniques including strace, ltrace, and LD\_PRELOAD.
* Utilize debuggers as an effective tools for dynamic analysis.

# 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-D2-Lecture.pptx

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

Lab Narrative: SRE-D2-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-D2-Lecture.pptx

**Lesson:** See SRE-D2-Lecture.pptx

**Active Learning Activity:** See SRE-D2-Lab.docx