Module B1: approaches to sre

**Module Description:** The intent of this module is to introduce the various goals for SRE (e.g., to determine how some piece of software works, to determine what vulnerabilities exist in the software, or to provide origination attribution) and general approaches to attacking SRE problems.

**Prerequisite Knowledge:** This module is intended to be a follow-up to Module A3: Forward Engineering.

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

**Level of Instruction:** This module intended to be an advanced 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 use SRE to investigate a collection of crackme files to determine what input is necessary to get the program to report that access is allowed. This will require you to select and execute an approach.

**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:

1. Explain at a high level various approaches to SRE tasks
2. Recognize and differentiate between the most common approaches to SRE tasks
3. Identify and evaluate the advantages and limitations of 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-B1-Lecture.pptx

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

Lab Narrative: SRE-B1-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-B1-Lecture.pptx

**Lesson:** See SRE-B1-Lecture.pptx

**Active Learning Activity:** See SRE-B1-Lab.docx