Module d5: Dynamic analysis for binary sre – Patching binaries.

**Module Description:** A common issue when performing dynamic analysis is getting components of the binary to execute (e.g., the binary may only perform some activity once per week, or only when it can contact a specific host on the Internet). As a result, it can be challenging to fully examine all aspects of the binary (particular in a timely manner). Binary patching can allow the analyst to modify the binary to ensure that components that are not executing do execute (e.g., a JZ instruction is changed to a JNZ, which results in a code path being taken instead of being skipped).This module will cover techniques for performing binary patching, and the limitations of those techniques.

**Prerequisite Knowledge:**  This is intended to be a follow-up to Module D4: Network Traffic Analysis.

**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 students patching binaries in order to execute code paths that are by default not executed.

**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:

* Identify the ways in which we can modify binaries.
* Differentiate (compare, analyze, annotate) between modification methods
* Explain why and when it might be strategic to modify binaries.

# 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-D5-Lecture.pptx

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

Lab Narrative: SRE-D5-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-D5-Lecture.pptx

**Lesson:** See SRE-D5-Lecture.pptx

**Active Learning Activity:** See SRE-D5-Lab.docx