Module d4: Dynamic analysis for binary sre – Network Traffic Analysis.

**Module Description:** This module will include coverage of network traffic analysis, and network service simulation, and C2 identification and analysis in the context of dynamic analysis of files of unknown origin and/or functionality. One common challenge is that dynamic analysis occurs in an isolated network environment, and binaries that interact with network services are prevented from doing so. This module will address approaches to that issue, in addition to reverse engineering C2 protocols by studying network traffic and its associated effects on the “compromised” host and its environment.

**Prerequisite Knowledge:** This is intended to be a follow-up to Module D3: Debuggers.

**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.

**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 giving students access to a host with an executing binary sample that is communicating with a C2 server (to which they do not have access). Students are required to reverse engineer the C2 network protocol based on dynamic analysis of the binary on the host, and any network traffic they choose to capture. Once they have determine what the C2 protocol is they are required to take control of the running binary using C2 commands.

**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 network traffic and explain the associated network concepts.
* Compare and assess methods for acquiring network traffic.
* Differentiate (compare, analyze, annotate) between network traffic types as they contribute to the SRE process.
* Explain how malicious network traffic can be hidden

# 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-D4-Lecture.pptx

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

Lab Narrative: SRE-D4-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-D4-Lecture.pptx

**Lesson:** See SRE-D4-Lecture.pptx

**Active Learning Activity:** See SRE-D4-Lab.docx