Studienarbeit: Reverse Engineering Lab

Studiengang Informatik
OST - Ostschweizer Fachhochschule
Campus Rapperswil Jon

Semester: Autumn 2022

Autors: Gianluca Nenz
Ronny Mueller
Thomas Kleb

Project Advisor: Ivan Buetler
Release: E-Prints
Version: Wednesday 12th October, 2022

School of Computer Science
OST Eastern Switzerland University of Applied Sciences

Abstract

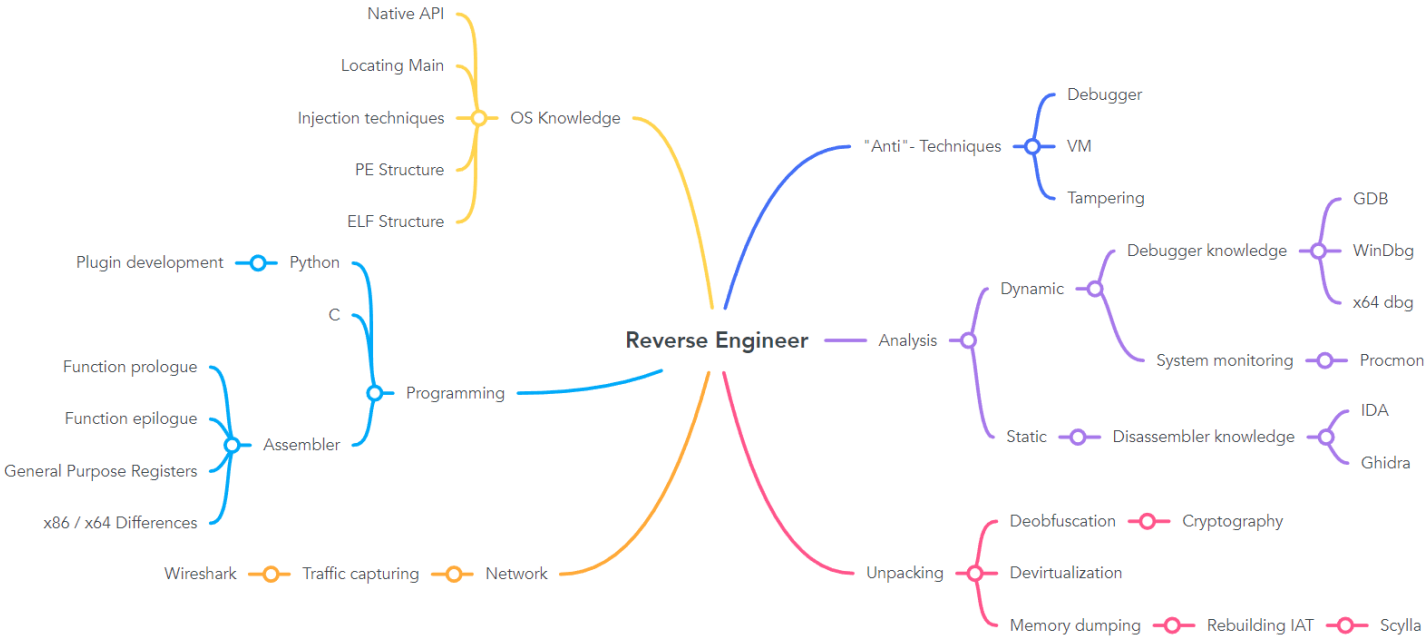
Contents

Chapter 1

Project Idea

1.1 Problem Domain

We defined in our opinion the most important domains which a Reverse Engineer has to have knowledge of.



1.2 Learning Concepts

Based on the Problem Domain from the last section we decided the most basic domains were programming, analysis and OS knowledge. So we decided that we are going to create the most labs and the first ones about these topics and then the later introduce the other domains in later Labs. We want to focus on Linux and Windows.

We also decided that we can expect for Students to already know about C, Python and some basic knowledge about Assembler because everyone has to have had BSYS which teaches about Assembler and C. Automation with python is also a module which now is in every sample curriculum at the OST.

Topic	Description
Debugging: Introduction	We intend to first explain the diffrence between static and dynamic debugging. We also plan to introduce the programs we are going to use with download links and additional information of how to use them. We also have a fast repetition of the most important assembler topics (registers, functions).
Static Debugging	Here we will tackle the first program for Linux and open it up in Ghidra or IDA. We will also provide a sample code on which the program is based on.
Dynamic Debugging	We will introduce the concept with the use of x64 dbg. In a simple excercise where you have to just patch some checks to get the flag.
Anti - Techniques	We explain the Anti-Techniques and show examples of them and how to deal with them.
Unpacking	We explain what Packing is, how to deal with it and specifically with devirtualization and deobfuscation.
Excercise Labs	This is the final Lab/Labs in which the students can use everything they learned in the previous chapters to solve excercises in different difficulties.

Chapter 2

Management Summary

Chapter 3

Product Documentation

Chapter 4

Project Documentation

Learning Concepts

Chapter 5

Meetings

5.1 06-10-22

Directory

Appendix

5.6 Eigenständigkeitserklärung

Eigenständigkeitserklärung

Erklärung
Wir erklären hiermit,

- dass wir die vorliegende Arbeit selbst und ohne fremde Hilfe durchgeführt haben, ausser derjenigen, welche explizit in der Aufgabenstellung erwähnt ist oder mit de Betreuer schriftlich vereinbart wurde,
- dass wir sämtliche verwendeten Quellen erwähnt und gemäss gängigen wissenschaftlichen Zitierregeln korrekt angegeben haben.
- dass wir keine duch Copyright geschützten Materialien (z.B. Bilder) in dieser Arbeit in unerlaubter Weise genutzt haben.

Gianluca Nenz	Date
Ronny Mueller	Date
Thomas Kleb	Date

5.7 Nutzungsrechte

5.8 Danksagung