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

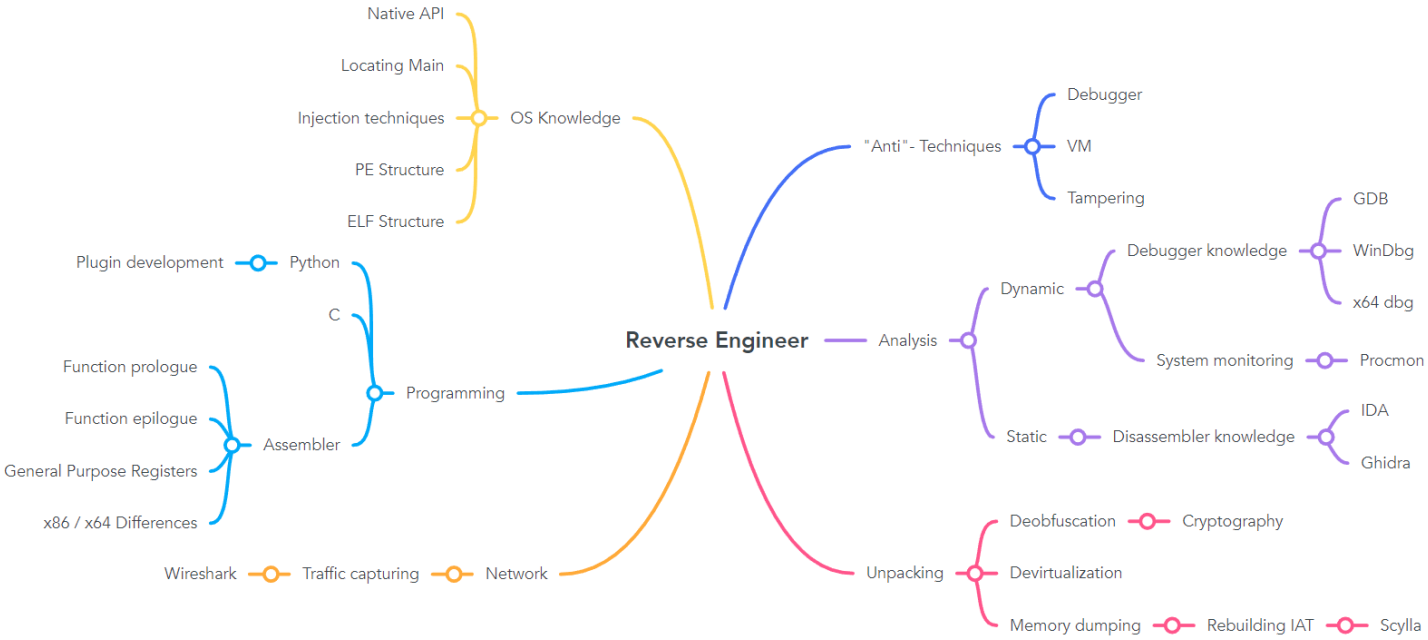
Contents

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
Refresher	Give the students some little refreshing on the key topics (Assembly)
Introduction to RE #1	Explain analysis approaches (Dynamic / Static) and install tools
Introduction to RE #2	Given a simple C file, students compile it and try to find a key (Static) (Find Main function)
Introduction to RE #3	Given a simple C file, students compile it and try to find a key (Dynamic) (learn GDB / x64)
First RE attempts	Given simple files compiled in several languages (PY, C#, C++) get flag
First keygen	Not only finding out the password but writing a keygen for the program
Harder CrackMes	Introduce new native API funcs / techniques like stack strings
Injection techniques	Explain some injection techniques
Dump memory	Explain how to dump memory off a given executable which uses a previously explained injection technique
"Anti"-Techniques	Introduce "Anti"-Techniques and provide program for students to bypass

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