LAB

6

Advance Dynamic Malware Analysis

By the end of this section of the practical, you should be able to:

- Understand how debugger is use in dynamic malware analysis
- Used the debugger tool to perform a dynamic analysis
- Investigate a sample program with a debugger

6.1 Introduction

Debuggers are one of the reverse engineering tools that enable analysist to execute a compiled program step by step, one step at a time. Analyst able to observe the instructions executed in which order, and which sections of the program are treated as code and which are treated as data. Debuggers help analysist to analyse the program while it is running, this allows analysist to get a better picture of what the program is executing during runtime

edb debugger is a Linux equivalent of the famous Olly debugger on the Windows platform. edb debugger can be used in investigating binary as it is executed. It is a powerful new way to write exploits, analyse malware, and reverse engineer binary files. It builds on a solid user interface with function graphing; the industry's first heap analysis tool built specifically for heap creation, and a large and well supported Python API for easy extensibility.

.

Task 1

Analysing Executable using edb Debugger

1. ***Analyse Puzzlesimple using edb Debugger***