The first step in learning reverse engineering is to familiarize yourself with the basics of assembly language and to learn how to use the debuggers to analyze an executable. GNU Debugger (GDB) is an open-source Linux/Unix compatible debugger that can be used for debugging programs written in languages such as Ada, C, C++, Objective C and Golang. The objective of this section is to cover the basics of GDB and how to use it to attach to processes and debug programs.

What will you learn?

- Basics of GDB Debugger
- Performing different operations with GDB

References:

1. GDB (https://www.gnu.org/software/gdb/)
2. GNU Debugger Megaprimer (https://www.pentesteracademy.com/course?id=4)
3. GDB Documentation (https://sourceware.org/gdb/current/onlinedocs/gdb)

Labs Covered:

- Running Processes Under GDB
  In this lab, you will learn to perform the basic operations in GDB. The following activities are covered under this lab:
  - Compiling the code
  - Running program
  - Passing Arguments
  - Environmental variables and Paths
  - Attaching to the running process
  - Multi-threaded program
  - Child Processes
  - Bookmarking

- Stopping and Continuing
  In this lab, you will learn to perform the basic operations in GDB. The following activities are covered under this lab:
  - Setting Breakpoints
  - Setting Watchpoints
  - Conditional Breakpoints
  - Saving and Importing Breakpoints
  - Dynamic printf
  - Continuing and stepping

- Recording/Replaying Inferior’s Execution
  In this lab, you will learn to perform the basic operations in GDB. The following activities are covered under this lab:
  - Record execution
  - Replay execution
  - Save it as a file
  - Load recorded execution

- Examining the Stack
  In this lab, you will learn to perform the basic operations in GDB. The following activities are covered under this lab:
  - Stack frames
  - Backtraces
  - Information on frame

- Editing source file
- Selecting the editor
- Specifying source directory
- Machine code

- Examining Data
  In this lab, you will learn to perform the basic operations in GDB. The following activities are covered under this lab:
  - Expressions
  - Program Variables
  - Output Formats
  - Examining Memory
  - Automatic Display
  - Print Settings
  - Convenience Variables
  - Registers
  - Vector Unit
  - Produce a Core File from Program

Running Processes Under GDB

Start

Stopping and Continuing

Start

Recording/Replaying Inferior's Execution

Start

Examining the Stack

Start

Examining Source Files

Start

Examining Data

Start