‹ Dashboard

STATIC BINARY ANALYSIS

Linux

Static Binary Analysis refers to the technique of analyzing a binary/program/application without executing it. The objective of the static analysis section would be to teach you how to use debuggers to carry out the static analysis of basic applications, and then how to reverse engineer the applications from the assembly code.

What will you learn?

- Static analysis of a binary using GDB
- Viewing/interpreting assembly code and examining data/registers

References:

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

Labs Covered:

- Recover Passcode
  In this lab, you will learn to analyze a binary using GDB and find a hardcoded passcode. The passcode is present in cleartext.

- Garbled Password
  In this lab, you will learn to analyze a binary using GDB and recover a password from it. The password is not present in the original form and needs to be derived.

- Caesar Protection
  In this lab, you will learn to analyze a binary using GDB and recover a password from it. The password present in encrypted form.

- We Love MD5
  In this lab, you will learn to analyze a binary using GDB and recover a password from it. The password needs to be derived using a famous one-way function.