ASSIGNMENT TITLE

# SUBJECT NAME: Cryptography and Network Security SUBJECT CODE: CS6008

# MODULE: 03

# NAME: R.Aadharsh

# REG.NO.: 2019103604

# DATE: 29/04/2022

**AIM:**

Implementing Return Oriented Programming(ROP)

**TOOLS INVOLVED:**

Linux , GDB , vim , gcc

**PROBLEM DESCRIPTION:**

Given a c code use ROP gadgets

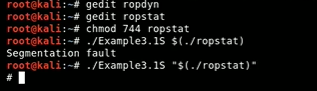
**INPUT:**

C code

**OUTPUT:**

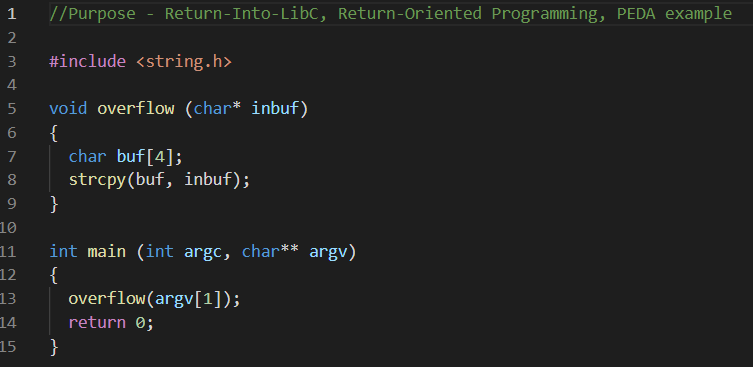
ROP implementation

**SCREENSHOT:**



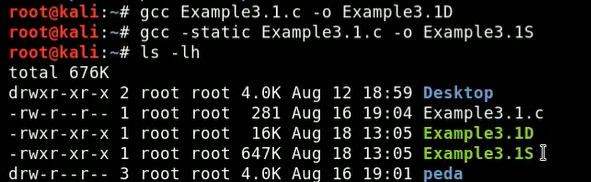
**C Code:**

Example3.1.c



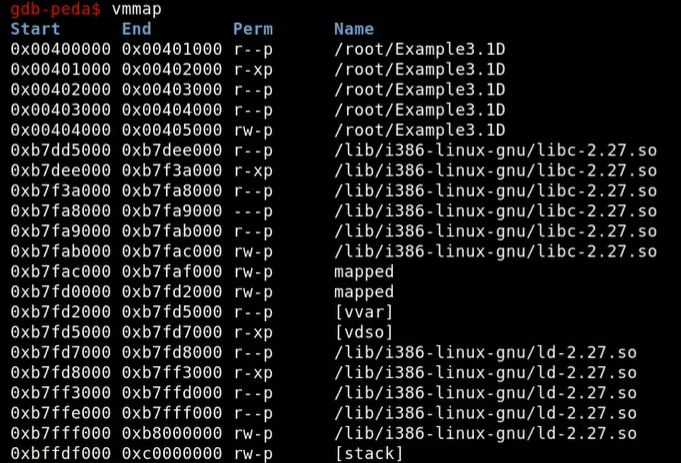
**Implementation:**

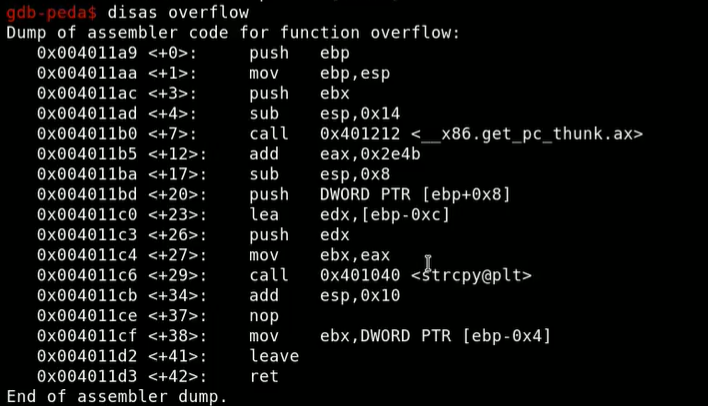
Compiling it dynamically and statically



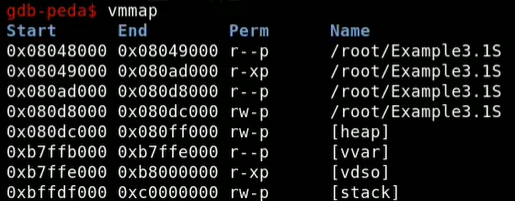
DYNAMIC VERSION:

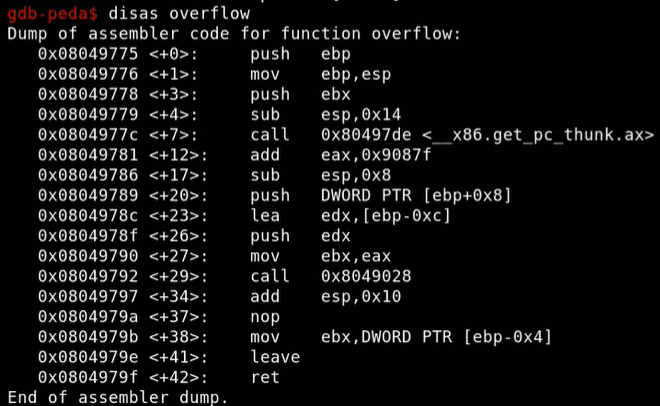
vmmap





STATIC VERSION:



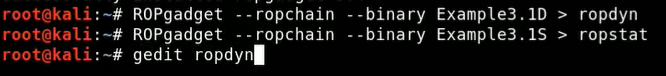


So static is clearly larger than dynamic compilation

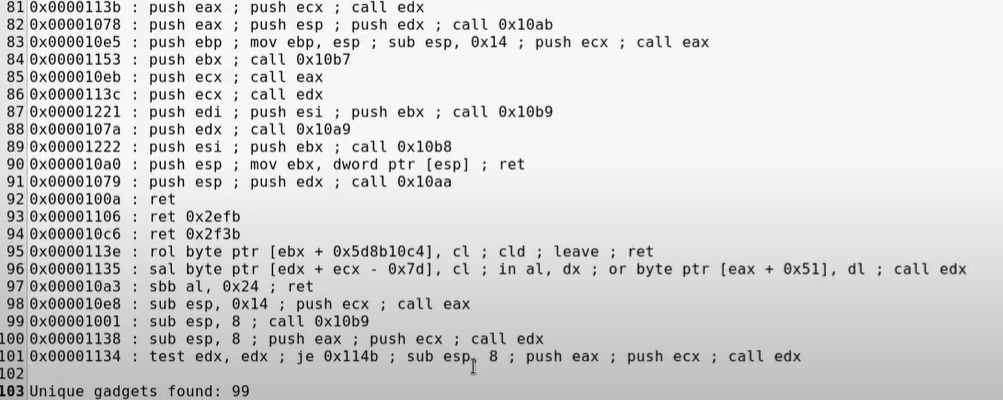
Installing rop gadget:



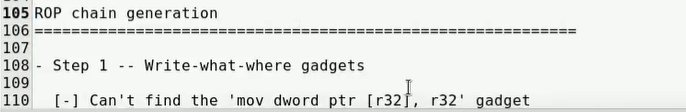
Using ropchain – binary and run it on both compile binaries



Ropdyn:

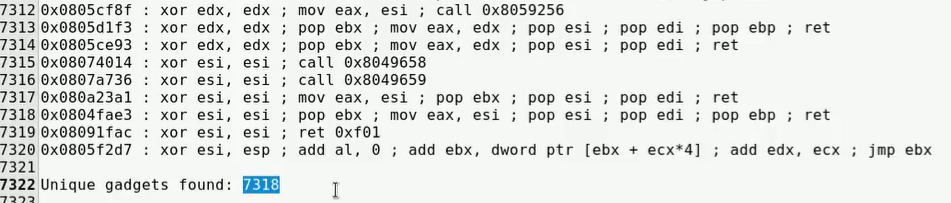


99 Unique gadgets are found

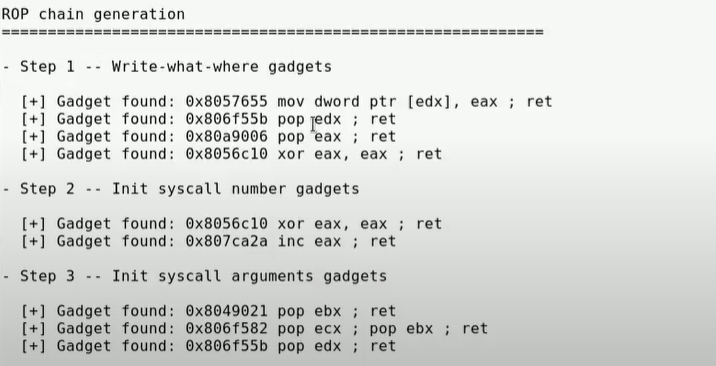


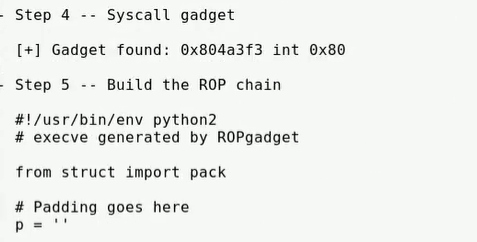
Failed to automatically detect ROP chain

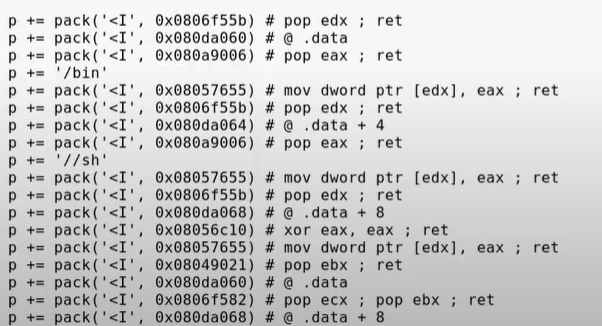
Ropstat:



7318 unique gadgets found

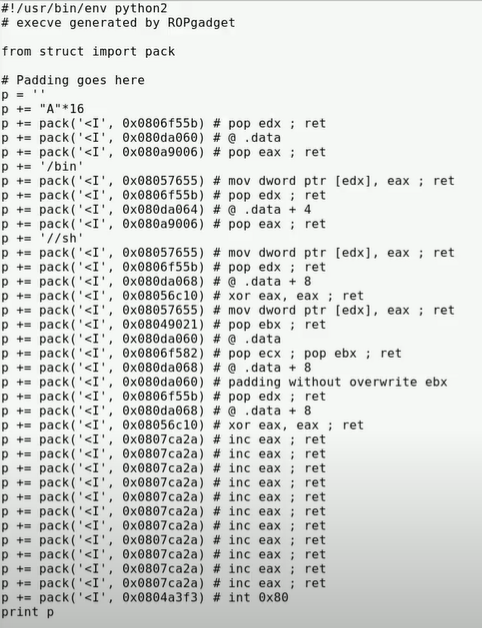






Successfully generated ROP chain

Delete everything from above python and removing the white space , as space matters in python and printing p which contains the concatenated rop chain



O/P:

