Reverse 0x02

ss8651twtw

Outline

- gdb
- ~~ida pro~~
- z3

GDB

套件安裝

- peda 安裝
  - https://github.com/longld/peda
- Pwngdb 安裝
  - https://github.com/scwuaptx/Pwngdb

套件安裝

- $ git clone https://github.com/longld/peda.git ~/peda
- $ echo "source ~/peda/peda.py" >> ~/.gdbinit
- $ git clone https://github.com/scwuaptx/Pwngdb.git
- $ ~/Pwngdb
- $ cp ~/Pwngdb/.gdbinit ~/

使用方法

- 執行 binary 並且使用 gdb 來 debug
  - $ gdb <binary>
- 先執行 gdb 之後再 attach 上要 debug 的 process
  - $ gdb
  - attach <pid>

GDB 指令

- 設定斷點
  - break <address>
  - break *0x0000000004004d7
- 執行程式
  - run

GDB 指令

- 執行下一個指令 (會追進 function)
  - step
- 執行下一個指令 (不會追進 function)
  - next

GDB 指令

- 繼續執行
  - continue
- 執行至 function 結束
  - finish

GDB 指令

- 跳轉
  - jump <address>
  - jump *0x0000000004004d7

GDB 指令

- 印出暫存器的值
  - print <register>
  - print $rax
- 印出記憶體的值
  - x <memory address>
  - x 0x7fffffffe920

GDB 指令

- 改變暫存器的值
  - set <register>=<value>
  - set $rsp=0x7fffffffe800
- 改變記憶體的值
  - set {<size>}<memory address>=<value>
  - set {int}0x7fffffffea00=2

LAB

- add
  - https://bamboofox.cs.nctu.edu.tw/courses/6/challenges/116
- guess
  - https://bamboofox.cs.nctu.edu.tw/courses/6/challenges/117

~~IDA Pro~~

反編譯大法

把 binary 反編譯回 C code

1. 在 functions window 點選想看的 function
2. 按下 F5
3. 完成!!!

字串表

列出可視字串表

- View => Open subviews => Strings
- shift + F12

標記

標記變數名

1. 先點擊要命名的變數
2. 按下 n
3. 輸入新的變數名

標記

標記 function 參數

1. 先點擊該 function
2. 按下 y
3. 輸入正確的 function 參數

標記

標記 struct 結構

1. 切到 Structures 頁面
2. 看裡面的說明
3. 新增 struct 並標記裡面的內容

標記

標記 struct 結構

```
; Ins/Del : create/delete structure
; D/A/*   : create structure member (data/ascii/array)
; N       : rename structure or structure member
; U       : delete structure member
```

LAB

- 2018 picoCTF
  - be-quick-or-be-dead-[123]
  - quackme
  - quackme up
  - keygen-me-1

Z3

Z3

- efficient SMT solver
- https://en.wikipedia.org/wiki/Satisfiability_modulo_theories
- https://github.com/Z3Prover/z3

安裝

- $ pip install z3-solver

測試一下

- $ python
- >>> from z3 import *

教學文件

- Z3 API in Python
- https://ericpony.github.io/z3py-tutorial/guide-examples.htm

解題步驟

- 定義未知量
- 添加約束條件
- 然後求解

範例

- x = Int('x')
- y = Int('y')
- solve(x > 2, y < 10, x + 2*y == 7)

範例

- p = Bool('p')
- q = Bool('q')
- r = Bool('r')
- solve(Implies(p, q), r == Not(q), Or(Not(p), r))

範例

- x, y, z = Reals('x y z')
- s = Solver()
- s.add(x > 1, y > 1, x + y > 3, z – x < 10)
- print s.check()
- m = s.model()
- print "x = %s" % m[x]

LAB

- 2018 picoCTF
  - keygen-me-2
  - circuit123