CTF Pwnable

Atum

About me

- Atum
  - CTF Player @Eur3kA @blue-lotus @Tea Deliverers
  - Master candidate @ICST SECLAB, Peking University
  - http://atum.li lgcpku@gmail.com
- Software Security
  - Focus on Vulnerability Discovering & Exploiting & Defense
  - Active in CTF, PWN/Reverse

CTF Pwnable Challenges Category

- Basic
- Reverse Engineering Related
- Standard Library Related
- Platform Related
- Real-world Scenarios
- Escaping
- Interesting Idea
- Guessing

Basic

- Easy Challenges use for warming up
- Examples
  - 33C3 CTF babyfengshui, grunt
  - 0CTF 2017 easiestprintf, diethard
  - 0CTF 2018 babystack
  - BKP CTF 2017 sss
  - DEFCON 25 qualifier beatthedl
  - HITCON CTF 2017 start

Reverse Engineering Related

- Once the reverse engineering was successfully completed, you got it
- Examples
  - Defcon 25 Qualifier resses revenge
  - Defcon 25 Final
  - Plaid CTF 2017 Plaid Party Planning
  - WCTF 2017 shellphish repeat VM
  - CodeGate CTF preliminary 2018 cpu
  - SECCON online CTF 2017 vm_no_fun
  - 0CTF 2018 Mighty Dragon

Platform Related

- You have to figure out the characteristic of specific platform
- Examples:
  - Defcon Finals
  - BKPCTF 2017 barewithme
  - SECCON CTF Final challenge2
  - N1CTF supersix's image kitchen
  - QWB CTF xx_fm_pwn

Standard Library Related

- You have to audit the source code to understand some specific internals of standard Library
- Examples
  - HITCON CTF 2017 babyfs
  - 0CTF 2018 heapstorm2
  - CodeGate CTF preliminary 2018 zoo
  - 34C3 CTF SimgeGC, 300, readme_revenge, v9
  - SECCON online CTF 2017 candyshop

Real World Scenarios

- Exploit Real World System or Software
- Examples
  - 34c3CTF LFA, babyvm, babyvm2, elgoog1, elgoog2, esprfs
  - 0CTF 2017 Final creadjar, babyqemu
  - 0CTF 2018 ZeroFS
  - HITCON CTF 2017 realrubyescape
  - Plaid CTF 2017 Chakrazy, Tetanus
  - WCTF 2017 babyfirstescape

Escaping

- Escaping sandbox or something
- Examples
  - 0CTF 2017 FINAL python
  - 0CTF 2018 blackhole
  - HITCON CTF 2018 rubyescape
  - BCTF 2017 BOJ
  - 33C3 CTF spacebox
  - seccon CTF 2017 FINAL OnlyOnceMemo

Interesting Idea

- Solving these challenges require you have some interesting thought
- Examples:
  - 33c3CTF ohfortuna, tea
  - BKPCTF2017 solitary confinement
  - HITCON CTF 2017 artifact
  - N1CTF 2017 trustworthy
  - BKP CTF 2017 hiddensec,

Guessing

- Just Guessing