PWN basic

Exploit

- 利用漏洞來達成攻擊
- 通常會希望達到任意代碼執行
- 又稱PWN

Exploit

- Flow
    - reverse engineering
    - find vulnerability
    - control flow
    - arbitrary code execution

Reverse Engineering

- Static analysis
  - objdump
  - IDA PRO
- Dynamic analysis
  - gdb

GDB

- Basic command
  - run (r)
  - break *0x8048014 (b)
  - info register (i r)
  - x/wx address
    - w 可換成 b/h/g 分別是取 1/2/8 byte
    - / 後可接數字表示一次列出幾個

GDB

- Basic command
    - ni
    - si
    - continue (c)
    - set *address=value
        - 將 address 中的值設成 value 一次設 4 byte
        - 可將 * 換成 {char/short/long} 分別設定 1/2/8 byte

GDB

- Basic command
  - attach pid
    - 可以配合 ncat 進行 exploit 的 debug
    - 需要root權限

Peda-GDB

- Python exploit development assistance for gdb
- https://github.com/longld/peda

Peda-GDB

- useful feature
  - checksec
  - vmmap
  - elfsymbol
  - readelf
  - find

Pwntool

- python exploit library
- https://github.com/Gallopsled/pwntools
- http://docs.pwntools.com/en/stable/

Pwntool

- r = remote(host, port)
    - r.recv(), r.recvline(), r.recvuntil()
    - r.send(), r.sendline()
- p = process(binary, env={})
    - 用法同上

Pwntool

- lib = ELF(elf_file)
  - lib.symbols[‘symbol’]
  - lib.search(str)
- p32(), p64(), u32(), u64()

ROPGadget

- useful tool to find rop gadget
- https://github.com/JonathanSalwan/ROPgadget
- ROPGadget --binary filename