

gdb调试 | pwndbg+pwndbg联合使用

原创

_n19hT

于 2020-04-21 00:54:36 发布

5567

★ 收藏 29

版权

分类专栏:

Linux

文章标签:

gdb



Linux 专栏收录该内容

0 订阅

18 篇文章

订阅专栏

文章目录

[前言](#)[pwngdb](#)[pwndbg](#)[pwngdb+pwndbg联合使用](#)

前言

好几天没熬夜了...为了搞几个gdb工具，我太难了。

pwngdb

pwngdb的功能特别广泛，主要如下

```
1 | libc : Print the base address of libc
2 | ld : Print the base address of ld
3 |
```

```
4 | codebase : Print the base of code segment
5 | heap : Print the base of heap
6 | got : Print the Global Offset Table infomation
7 | dyn : Print the Dynamic section infomation
8 | findcall : Find some function call
9 | bcall : Set the breakpoint at some function call
10 | tls : Print the thread local storage address
11 | at : Attach by process name
12 | findsyscall : Find the syscall
13 | fmtarg : Calculate the index of format string
14 | You need to stop on printf which has vulnerability.
15 | force : Calculate the nb in the house of force.
16 | heapinfo : Print some infomation of heap
17 | heapinfo (Address of arena)
18 | default is the arena of current thread
19 | If tcache is enable, it would show infomation of tcache entry
20 | heapinfoall : Print some infomation of heap (all threads)
21 | arenainfo : Print some infomation of all arena
22 | chunkinfo: Print the infomation of chunk
23 | chunkinfo (Address of victim)
```

安装教程:

```
1 | cd ~/
2 | git clone https://github.com/scwuaptx/Pwngdb.git
3 | cp ~/Pwngdb/.gdbinit ~/
```

pwndbg

安装教程:

```
1 | git clone https://github.com/pwndbg/pwndbg
2 | cd pwndbg
3 | ./setup.sh
```

这个和上面的可不一样...区别还是挺大的。pwndbg是我一直以来使用的比较顺手的gdb工具，界面好看，而且命令实用。做格式化字符串题目的时候使用到了pwntools里面的 **fmtstr_payload()**，其中要传一个参数就是格式化字符串的offset，而在**pwngdb**里面有个**fmtarg工具**可以直接算出这个offset！**所以要pwndbg配合pwngdb使用！**

pwngdb+pwndbg联合使用

我也是第一次知道pwngdb还能附加到pwndbg上面使用...调试花了我好几个小时。

坑1:

在home目录下的.gdbinit文件里面是没有pwndbg信息的(如果安装的时候没写进去的话)

```
1 | vim ~/.gdbinit
2 | 然后写入
3 | source ~/pwndbg/gdbinit.py
```

```
1 #source ~/peda/peda.py
2 source ~/pwndbg/gdbinit.py
3 source ~/Pwngdb/pwngdb.py
4 source ~/Pwngdb/angelheap/gdbinit.py
5
6 define hook-run
7 python
8 import angelheap
9 angelheap.init_angelheap()
10 end
11 end
```

一定要把这条放在第4条前面
不然gdb就会默认是pwngdb

下面三条都不能注释,
不然pwndbg可以用
但是用不了pwngdb
里面的功能

https://blog.csdn.net/weixin_43092232

```
1c devil@ubuntu:~/adworld/pwn/data-detection$ gdb -q data_detection
pwndbg: loaded 181 commands. Type pwndbg [filter] for a list.
0 pwndbg: created $rebase, $ida gdb functions (can be used with print/break)
1 Reading symbols from data_detection...(no debugging symbols found)...done.
2 pwndbg> fmtarg
Python Exception <class 'gdb.error'> The program has no registers now.:
g> Python Exception <class 'gdb.error'> Error occurred in Python command: The progr
g> am has no registers now.:
Error occurred in Python command: Error occurred in Python command: The program
has no registers now.
pwndbg>
```

默认是pwndbg

可以使用pwngdb工具

https://blog.csdn.net/weixin_43092232

附:

fmtarg运用实例