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

文章目录

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

```
libc : Print the base address of libc
ld : Print the base address of ld

```

```
codebase : Print the base of code segment
heap : Print the base of heap
got : Print the Global Offset Table infomation
dyn : Print the Dynamic section infomation
findcall : Find some function call
bcall : Set the breakpoint at some function call
tls : Print the thread local storage address
at : Attach by process name
findsyscall : Find the syscall
fmtarg : Calculate the index of format string
You need to stop on printf which has vulnerability.
force : Calculate the nb in the house of force.
heapinfo : Print some infomation of heap
heapinfo (Address of arena)
default is the arena of current thread
If tcache is enable, it would show infomation of tcache entry
heapinfoall : Print some infomation of heap (all threads)
arenainfo : Print some infomation of all arena
chunkinfo: Print the infomation of chunk
chunkinfo (Address of victim)
```

安装教程:

```
cd ~/
git clone https://github.com/scwuaptx/Pwngdb.git
cp ~/Pwngdb/.gdbinit ~/
```

pwndbg

安装教程：

```
git clone https://github.com/pwndbg/pwndbg
cd pwndbg
./setup.sh
```

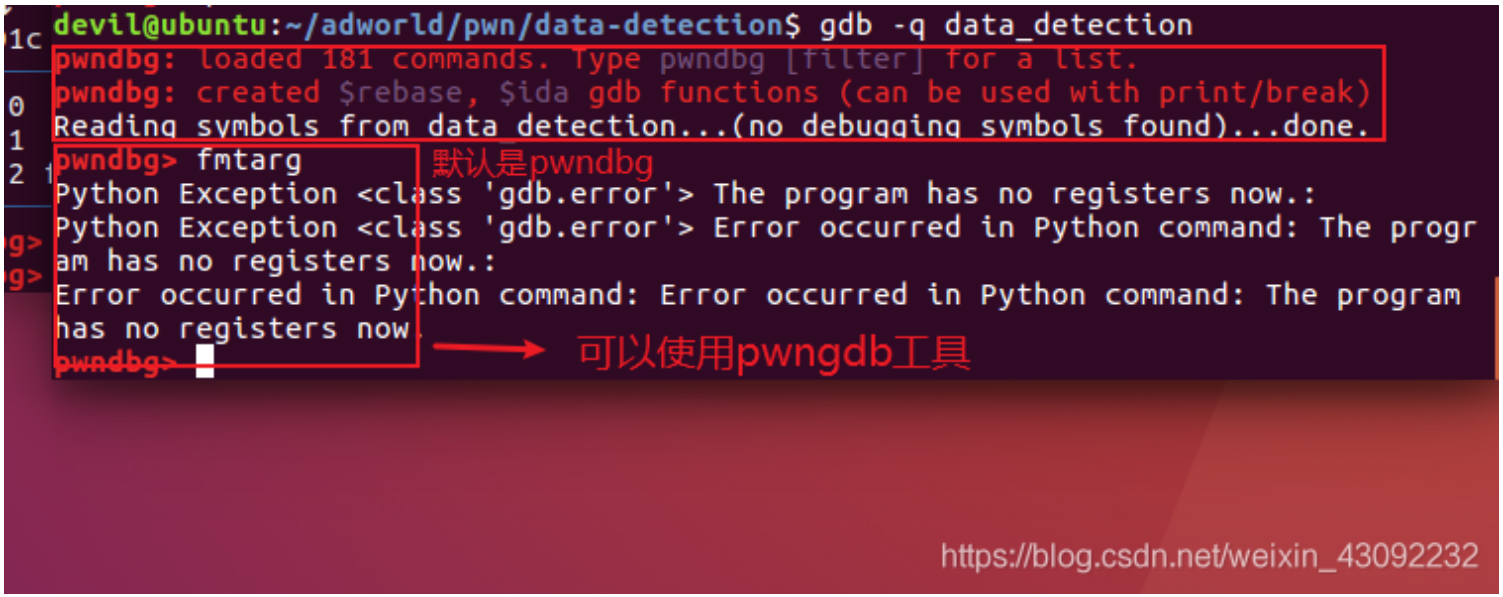
这个和上面的可不一样…区别还是挺大的。pwndbg是我一直以来使用的比较顺手的gdb工具，界面好看，而且命令实用。做格式化字符串题目的时候使用到了pwntools里面的 **fmtstr_payload()**，其中要传一个参数就是格式化字符串的offset，而在**pwngdb**里面有个**fmtarg工具**可以直接算出这个offset！**所以要pwndbg配合pwngdb使用！**

---

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)

```
vim ~/.gdbinit
然后写入
source ~/pwndbg/gdbinit.py
```



附:

fmtarg运用实例