pwnable.kr 4.flag writeup

原创

dittozzz 于 2018-12-15 20:31:53 发布 430 收藏

分类专栏： pwn 文章标签： pwn

没涉及到pwn，就是一道逆向题目。
拿到题目

Papa brought me a packed present! let's open it.

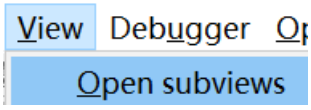
Download : http://pwnable.kr/bin/flag

This is reversing task. all you need is binary

访问 http://pwnable.kr/bin/flag 下载文件。。
用IDA打开查看汇编代码。

```
loc_44A516:                             ; CODE
                mov     ebx, [rsi]
                sub     rsi, 0FFFFFFFFFFFFFFFCh
                adc     ebx, ebx
                mov     dl, [rsi]
                rep retn
start           endp ; sp-analysis failed
```

发现加了壳，打开字符串窗口看看有没有信息，（shift 加上f12快捷键打开，或者



在这里找到字符串窗口并打开，

```
LOAD:000…  00000005     C     '_(H
LOAD:000…  00000005     C     USQRH
LOAD:000…  0000001E     C     PROT_EXEC|PROT_WRITE
LOAD:000…  0000004F     C     $Info: This file is
LOAD:000…  0000004C     C     $Id: UPX 3.08 Copyr
```

随便一翻就看到了关键字upx，看来应该是upx的壳，用linux下自带的upx脱壳尝试下，

```
wxy@ubuntu:~$ cd Desktop/
wxy@ubuntu:~/Desktop$ upx -d flag.elf
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2017
UPX 3.94        Markus Oberhumer, Laszlo Molnar & John

        File size         Ratio      Format      Name
   --------------------   ------   -----------   ------
    883745 <-    335288   37.94%   linux/amd64   flag.e

Unpacked 1 file.
```


脱壳成功。再用IDA打开，点开main函数，f5查看伪代码，

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char *dest; // ST08_8

  puts("I will malloc() and strcpy the flag there. take it.", argv, envp);
  dest = (char *)malloc(100LL);
  strcpy(dest, flag);
  return 0;
}
```



```
aUpxSoundsLikeA db 'UPX...? sounds like a delivery service :)',0
```

点开flag，得到flag