BUUCTF Reverse/[ACTF新生赛2020]easyre

原创

这就是强者的世界么 于 2021-07-19 10:39:21 发布 4660 收藏

分类专栏： # BUUCTF Reverse

本文链接：https://blog.csdn.net/ookami6497/article/details/118890020

版权

BUUCTF Reverse 专栏收录该内容

58 篇文章 2 订阅

订阅专栏

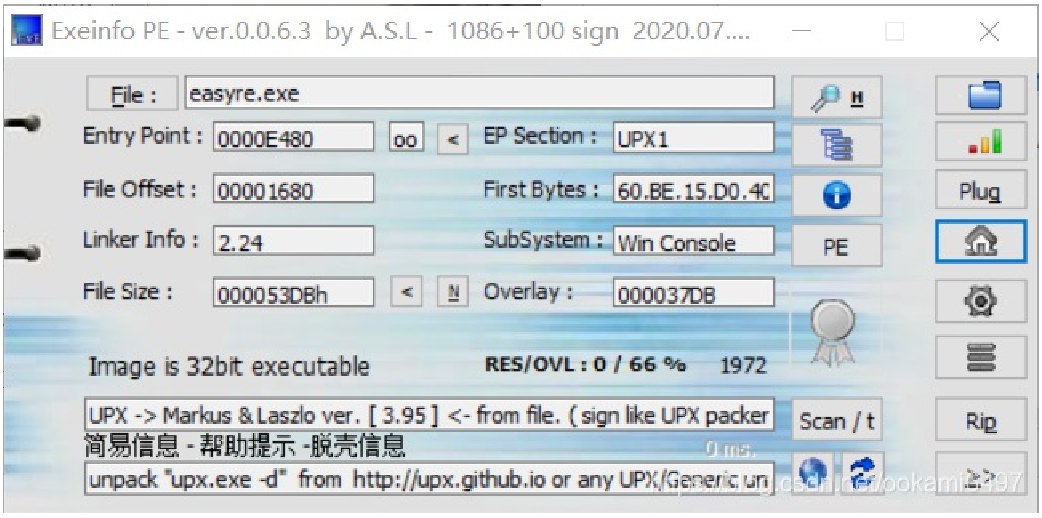
BUUCTF Reverse/[ACTF新生赛2020]easyre

[ACTF新生赛2020]easyre

1

得到的 flag 请包上 flag{} 提交。

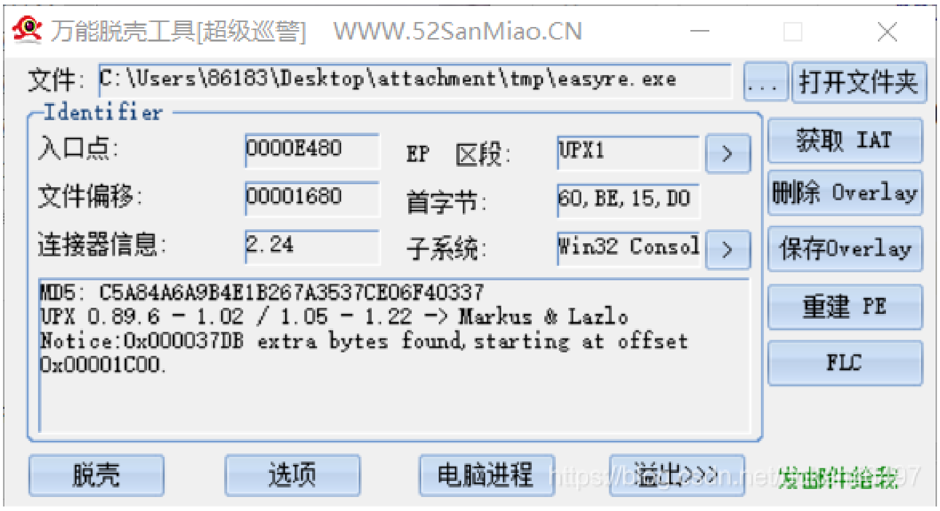
> 发现UPX壳



Exeinfo PE - ver.0.0.6.3 by A.S.L - 1086+100 sign 2020.07....

File : easyre.exe
Entry Point : 0000E480 oo < EP Section : UPX1
File Offset : 00001680 First Bytes : 60.BE.15.D0.4C
Linker Info : 2.24 SubSystem : Win Console
File Size : 000053DBh < N Overlay : 000037DB
Image is 32bit executable RES/OVL : 0 / 66 % 1972
UPX -> Markus & Laszlo ver. [3.95] <- from file. (sign like UPX packer
简易信息 - 帮助提示 -脱壳信息 0 ms.
unpack "upx.exe -d" from http://upx.github.io or any UPX/Generic un

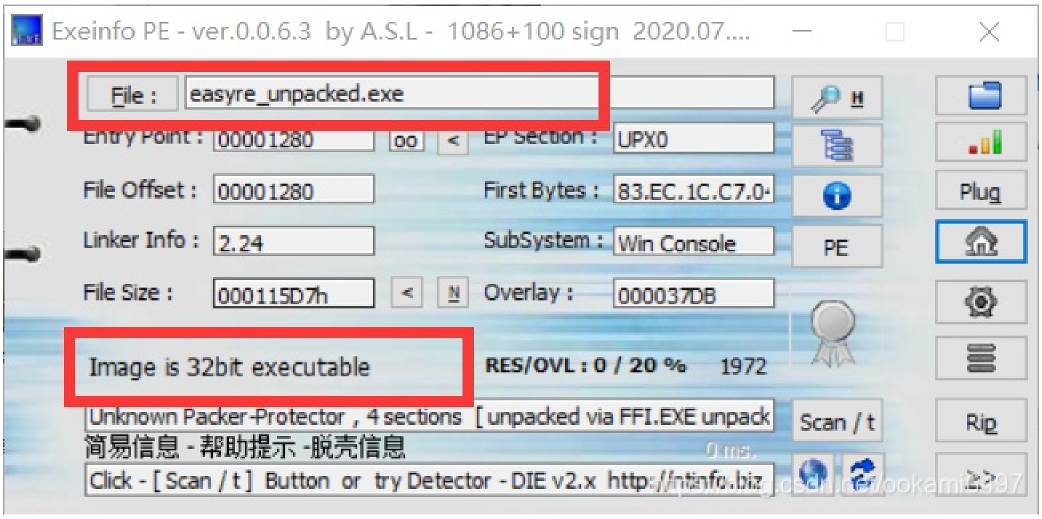
进行脱壳



万能脱壳工具[超级巡警] WWW.52SanMiao.CN

文件: C:\Users\86183\Desktop\attachment\tmp\easyre.exe
Identifier
入口点: 0000E480 EP 区段: UPX1
文件偏移: 00001680 首字节: 60, BE, 15, D0
连接器信息: 2.24 子系统: Win32 Consol

```
MD5: C5A84A6A9B4E1B267A3537CE06F40337
UPX 0.89.6 - 1.02 / 1.05 - 1.22 -> Markus & Lazlo
Notice:0x000037DB extra bytes found,starting at offset
0x00001C00.
```



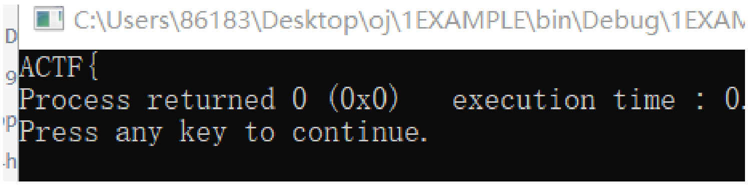
Exeinfo PE - ver.0.0.6.3 by A.S.L - 1086+100 sign 2020.07....

File : easyre_unpacked.exe
Entry Point : 00001280 oo < EP Section : UPX0
File Offset : 00001280 First Bytes : 83.EC.1C.C7.04
Linker Info : 2.24 SubSystem : Win Console
File Size : 000115D7h < N Overlay : 000037DB
Image is 32bit executable RES/OVL : 0 / 20 % 1972
Unknown Packer-Protector , 4 sections [unpacked via FFI.EXE unpack
简易信息 - 帮助提示 -脱壳信息 0 ms.
Click - [Scan / t] Button or try Detector - DIE v2.x http://ntinfo.biz

用IDA32位打开，找到main函数进行分析

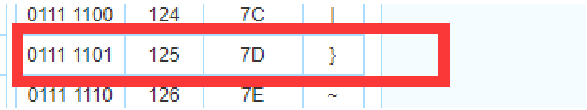
```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  _BYTE v4[12]; // [esp+12h] [ebp-2Eh] BYREF
  _DWORD v5[3]; // [esp+1Eh] [ebp-22h]
  _BYTE v6[5]; // [esp+2Ah] [ebp-16h] BYREF
  int v7; // [esp+2Fh] [ebp-11h]
  int v8; // [esp+33h] [ebp-Dh]
  int v9; // [esp+37h] [ebp-9h]
  char v10; // [esp+3Bh] [ebp-5h]
  int i; // [esp+3Ch] [ebp-4h]

  sub_401A10();
  qmemcpy(v4, "*F'\"N,\"(I?+@", sizeof(v4));
  printf("Please input:");
  scanf("%s", v6);
  if ( v6[0] != 65 || v6[1] != 67 || v6[2] != 84 || v6[3] != 70 || v6[4] != 123 || v10 != 125 )
    return 0;
  v5[0] = v7;
  v5[1] = v8;
  v5[2] = v9;
  for ( i = 0; i <= 11; ++i )
  {
    if ( v4[i] != byte_402000[*((char *)v5 + i) - 1] )
      return 0;
  }
  printf("You are correct!");
  return 0;
}
```

> 将v6转成字符看看，得到ACTF{



```
C:\Users\86183\Desktop\oj\1EXAMPLE\bin\Debug\1EXAM
ACTF{
Process returned 0 (0x0)   execution time : 0.
Press any key to continue.
```

> 看一下v10的值，v10 = }

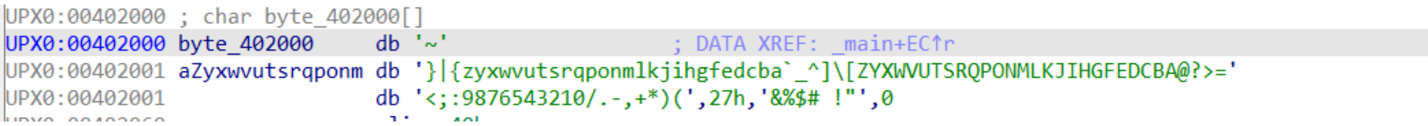


0111 1100	124	7C	|
0111 1101	125	7D	}
0111 1110	126	7E	~

> 看到for循环，推测flag在v5中

```
for ( i = 0; i <= 11; ++i )
 {
   if ( v4[i] != byte_402000[*((char *)v5 + i) - 1] )
     return 0;
 }
```

> 跟进byte_402000，注意看清楚逗号



```
UPX0:00402000 ; char byte_402000[]
UPX0:00402000 byte_402000     db '~'                  ; DATA XREF: _main+EC↑r
UPX0:00402001 aZyxwvutsrqponm db '}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>='
UPX0:00402001                 db '<;:9876543210/.-,+*)(',27h,'&%$# !"',0
```

注意

从for循环条件中推出flag为12位，但是v4长度有14位。注意v4中的 \" ,这是c语言中的转义字符，只代表一个 "

```
for ( i = 0; i <= 11; ++i )
 {
   if ( v4[i] != byte_402000[*((char *)v5 + i) - 1] )
     return 0;
 }
```

```
 qmemcpy(v4, "*F'\"N,\"(I?+@", sizeof(v4));
```

所以得到（在python中字符串有三种表现形式，三个单引号（'''）、双引号（"）、单引号（'））

```
v4 = '''*F'"N,"(I?+@'''
```

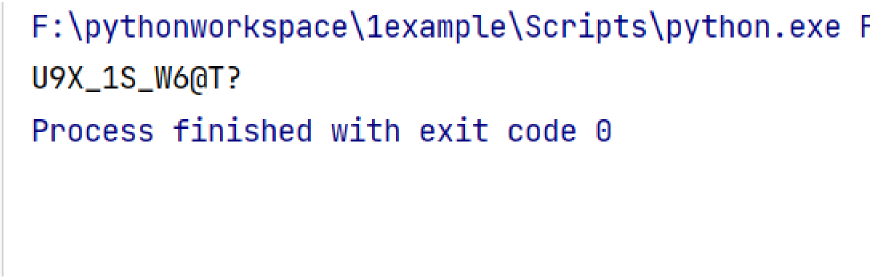
然后得到（python中 \ 要用 \\ 表示，详情请看这个Python中关于反斜杠（\）用法的总结）

```
by = '''~}|{zyxwvutsrqponmlkjihgfedcba`_^]\\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>=<;:9876543210/.-,+*)
```

然后写出脚本

```
by = '''~}|{zyxwvutsrqponmlkjihgfedcba`_^]\\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>=<;:9876543210/.-,+*)('&%$# !"'''
v4 = '''*F'"N,"(I?+@'''

for i in range(len(v4)):
    for j in range(len(by)):
        if  v4[i] == by[j]:
            #print("v5[{}] - 1 = {} ,v5[{}] = {} ".format(i,j,i,chr(j + 1)))
            print(chr(j + 1),end = '')
```

运行得到结果



```
F:\pythonworkspace\1example\Scripts\python.exe F
U9X_1S_W6@T?
Process finished with exit code 0
```