BUUCTF Reverse [ACTF新生赛2020]easyre WriteUp

原创

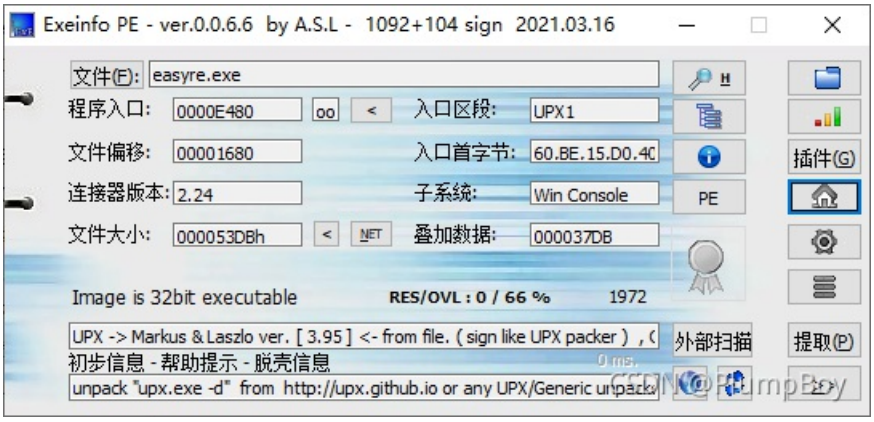
PlumpBoy 于 2021-09-11 16:15:23 发布 62 收藏

分类专栏： BUUCTF 逆向题解 文章标签： 系统安全 安全

本文链接：https://blog.csdn.net/weixin_45723661/article/details/120228117

easyre-WP

打开后先查查有无壳，发现是UPX加密



kali直接脱壳，命令为`upx -d easyre.exe`

脱完壳直接放入IDA查看反汇编代码

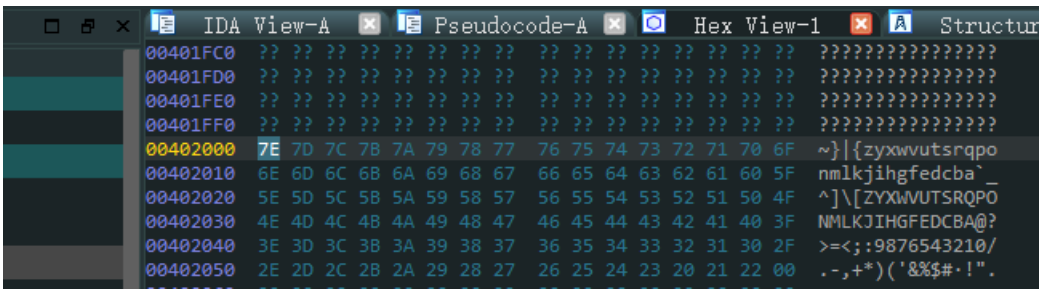
```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  _BYTE v4[12]; // [esp+12h] [ebp-2Eh] BYREF
  _DWORD v5[3]; // [esp+1Eh] [ebp-22h]
  _BYTE v6[5]; // [esp+2Ah] [ebp-16h] BYREF
  int v7; // [esp+2Fh] [ebp-11h]
  int v8; // [esp+33h] [ebp-Dh]
  int v9; // [esp+37h] [ebp-9h]
  char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

  __main();
  qmemcpy(v4, "*F'\"N,\"(I?+@", sizeof(v4)); //注意转义符号
  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] != _data_start__[*((char *)v5 + i) - 1] )
      return 0;
  }
  printf("You are correct!");
  return 0;
}
```

_data_start__为：

```
.data:00402000                 public __data_start__
.data:00402000 ; char _data_start__[]
.data:00402000 __data_start__  db 7Eh                 ; DATA XREF: _main+ECtr
.data:00402001 aZyxwvutsrqponm db '}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>='
.data:00402001                 db '<;:9876543210/.-,+*)(',27h,'&%$# !"',0
.data:00402060                 align 40h
.data:00402080                 public __CRT_glob
.data:00402080 __CRT_glob      dd 0FFFFFFFFh          ; DATA XREF: ___mingw_CRTStartup+4Atr
```

但是此处注意，最上面的7E也要算，所以建议在HexView视图中查看。



通过阅读代码我们可以得知，其要做的就是在_data_start__中找到v4中的字符，而这个索引值就是v5中的数据，也就是flag，写出解密脚本

```
a = '~}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>=<;:9876543210/.-,+*)(\'&%$# !"'
bnum = [42,70,39,34,78,44,34,40,73,63,43,64]
x=[]
flag=''
for i in bnum:
    x.append(a.find(chr(i))+1)
for i in x:
    flag+=chr(i)

print(flag)
```

最终得到`U9X_1S_W6@T?`