攻防世界 Reverse高手进阶区 3分题 EASYHOOK

原创

思源湖的鱼 于 2021-01-19 17:04:19 发布 232 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 reverse

本文链接：https://blog.csdn.net/weixin_44604541/article/details/112797499

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Reverse高手进阶区的3分题

本篇是EASYHOOK的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

PE查壳

扔进IDA

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int result; // eax
  HANDLE v4; // eax
  DWORD NumberOfBytesWritten; // [esp+4h] [ebp-24h]
  char Buffer; // [esp+8h] [ebp-20h]

  sub_401370(aPleaseInputFla);
  scanf(a31s, &Buffer);
  if ( strlen(&Buffer) == 19 )
  {
    sub_401220();
    v4 = CreateFileA(FileName, 0x40000000u, 0, 0, 2u, 0x80u, 0);
    WriteFile(v4, &Buffer, 0x13u, &NumberOfBytesWritten, 0);
    sub_401240(&Buffer, &NumberOfBytesWritten);
    if ( NumberOfBytesWritten == 1 )
      sub_401370(aRightFlagIsYou);
    else
      sub_401370(aWrong);
    system(aPause);
    result = 0;
  }
  else
  {
    sub_401370(aWrong);
    system(aPause);
    result = 0;
  }
  return result;
}
```


sub_401370显然是个输出

看sub_401220和sub_401240

```
signed int __cdecl sub_401240(const char *a1, _DWORD *a2)
{
  signed int result; // eax
  unsigned int v3; // kr04_4
  char v4[24]; // [esp+Ch] [ebp-18h]

  result = 0;
  strcpy(v4, "This_is_not_the_flag");
  v3 = strlen(a1) + 1;
  if ( (signed int)(v3 - 1) > 0 )
  {
    while ( v4[a1 - v4 + result] == v4[result] )
    {
      if ( ++result >= (signed int)(v3 - 1) )
      {
        if ( result == 21 )
        {
          result = (signed int)a2;
          *a2 = 1;
        }
        return result;
      }
    }
  }
  return result;
}
```



```
int sub_401220()
{
  HMODULE v0; // eax
  DWORD v2; // eax

  v2 = GetCurrentProcessId();
  hProcess = OpenProcess(0x1F0FFFu, 0, v2);
  v0 = LoadLibraryA(LibFileName);
  dword_40C9C4 = (int)GetProcAddress(v0, ProcName);
  lpAddress = (LPVOID)dword_40C9C4;
  if ( !dword_40C9C4 )
    return sub_401370((int)&unk_40A044);
  unk_40C9B4 = *(_DWORD *)lpAddress;
  *((_BYTE *)&unk_40C9B4 + 4) = *((_BYTE *)lpAddress + 4);
  byte_40C9BC = -23;
  dword_40C9BD = (char *)sub_401080 - (char *)lpAddress - 5;
```

```
  return sub_4010D0();
}
```



```
int __stdcall sub_401080(HANDLE hFile, LPCVOID lpBuffer, DWORD nNumberOfBytesToWrite, LPDWORD lpNumberOfBytesWritten, LPOVERLAPPED lpOverlapped)
{
  signed int v5; // ebx

  v5 = sub_401000((int)lpBuffer, nNumberOfBytesToWrite);
  sub_401140();
  WriteFile(hFile, lpBuffer, nNumberOfBytesToWrite, lpNumberOfBytesWritten, lpOverlapped);
  if ( v5 )
    *lpNumberOfBytesWritten = 1;
  return 0;
}
```

```
signed int __cdecl sub_401000(int a1, signed int a2)
{
  char v2; // al
  char v3; // bl
  char v4; // cl
  int v5; // eax

  v2 = 0;
  if ( a2 > 0 )
  {
    do
    {
      if ( v2 == 18 )
      {
        *(_BYTE *)(a1 + 18) ^= 0x13u;
      }
      else
      {
        if ( v2 % 2 )
          v3 = *(_BYTE *)(v2 + a1) - v2;
        else
          v3 = *(_BYTE *)(v2 + a1 + 2);
        *(_BYTE *)(v2 + a1) = v2 ^ v3;
      }
      ++v2;
    }
    while ( v2 < a2 );
  }
  v4 = 0;
  if ( a2 <= 0 )
    return 1;
  v5 = 0;
  while ( byte_40A030[v5] == *(_BYTE *)(v5 + a1) )
  {
    v5 = ++v4;
    if ( v4 >= a2 )
      return 1;
  }
  return 0;
}
```



```
.data:0040A030 byte_40A030     db 61h                  ; DATA XREF: sub_401000:loc_401051↑r
.data:0040A031                 db  6Ah ; j
.data:0040A032                 db  79h ; y
.data:0040A033                 db  67h ; g
.data:0040A034                 db  6Bh ; k
.data:0040A035                 db  46h ; F
.data:0040A036                 db  6Dh ; m
.data:0040A037                 db  2Eh ; .
.data:0040A038                 db  7Fh ;
.data:0040A039                 db  5Fh ; _
.data:0040A03A                 db  7Eh ; ~
.data:0040A03B                 db  2Dh ; -
.data:0040A03C                 db  53h ; S
.data:0040A03D                 db  56h ; V
.data:0040A03E                 db  7Bh ; {
.data:0040A03F                 db  38h ; 8
.data:0040A040                 db  6Dh ; m
.data:0040A041                 db  4Ch ; L
.data:0040A042                 db  6Eh ; n
.data:0040A043                 db    0
```

```
.data:0040C9A4 dword_40C9A4    dd 1E0h                 ; DATA XREF: sub_403BA6:loc_403BE2↑r
.data:0040C9A4                                         ; sub_4040AA+51↑r ...
.data:0040C9A8                 align 10h
.data:0040C9B0 ; LPVOID lpAddress
.data:0040C9B0 lpAddress       dd 0                    ; DATA XREF: sub_4010D0+3↑r
.data:0040C9B0                                         ; sub_4010D0+2B↑r ...
```

发现加密函数其实是401000

```
dic=[0x61, 0x6A, 0x79, 0x67, 0x6B, 0x46, 0x6D, 0x2E, 0x7F, 0x5F, 0x7E, 0x2D,
0x53, 0x56, 0x7B, 0x38, 0x6D, 0x4C, 0x6E]
flag=list("------------------")
flag[-1]=chr(dic[-1]^0x13)
for i in range(17,-1,-1):
 tmp=dic[i]^i
 if i%2==1:
  flag[i]=chr(tmp+i)
 else:
  flag[i+2]=chr(tmp)
print(''.join(flag))
```

```
1  dic=[0x61, 0x6A, 0x79, 0x67, 0x6B, 0x46, 0x6D, 0x2E, 0x7F, 0x5F, 0x7E, 0x2D,
2  0x53, 0x56, 0x7B, 0x38, 0x6D, 0x4C, 0x6E]
3  flag=list("------------------")
4  flag[-1]=chr(dic[-1]^0x13)
5  for i in range(17,-1,-1):
6      tmp=dic[i]^i
7      if i%2==1:
8          flag[i]=chr(tmp+i)
9      else:
10         flag[i+2]=chr(tmp)
11 print(''.join(flag))
```

```
-lag{Ho0k_w1th_Fun}
```


得到flag

结语

关键是找到加密函数