【逆向学习】暗号 writeup

原创

charlie_heng 于 2017-12-20 13:25:49 发布 587 收藏

分类专栏： 二进制-逆向工程

本文链接：https://blog.csdn.net/charlie_heng/article/details/78852124

这是16年国赛的一道题，以前做过一次，现在又重新做一下，做完这题感觉到。。。单纯靠脑子来跑程序真心不可靠，还是copy下再run下观察结果来得实际点

首先看下check函数

```
v4 = a4;
v11 = a2;
v5 = a1;
v10 = (char *)(*(int (**)(void))(*a1 + 676))();
v6 = (const char *)(*(int (__fastcall **)(int *, int, _DWORD))(*v5 + 676))(v5, v4, 0);
memset(&s, 0, 0x40u);
if ( WeAreTheChangPingPeople() == 1 )
  v9 = NowYouSeeMe(v10, v6);
if ( v9 )
  strcpy(&s, "What a pity!!");
else
  strcat(&s, "You got it! The target is 9527");
memset(&dest, 0, 0xC8u);
strcpy(&dest, "/proc/net/tcp");
v7 = fopen(&dest, "rb");
if ( !v7 )
  exit(-1);
while ( fgets(&dest, 200, v7) )
{
  if ( strstr(&dest, ":5D8A") )
    strcpy(&s, "Why so serious...");
}
fclose(v7);
sleep(1u);
AtLeastWeStoleTheShow((unsigned int)&s, v5, v11);
return 0;
```


在WeAretheChangPingPeople这个函数里面，在5555端口监听信息，然后与hhxptgdlffojwztpewc比较

接下来看下NowYouSeeMe这个函数

开头的一大段连接5555端口之类的就不看了，我们来看下主要的部分

```
while ( v12 < v27 )
{
  sprintf(&s1[3 * v12], "%03d", (unsigned __int8)dest[v12]);
  ++v12;
}
printf("%s\n", v40);
memset(&v35, 0, 0x32u);
strcpy(
  &s2,
  "000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000"
  "0000000000000000000000000000000000000000000000000");
v13 = 0;
v14 = 0;
n = 3 * v27;
while ( 1 )
{
  while ( v14 < v27 )
  {
    v29 = 3 * v14;
    v15 = 100 * (unsigned __int8)s1[3 * v14] + 1000 * v13;
    v16 = 3 * v14++;
    v28 = &s1[v16];
    v17 = v15 + 10 * (unsigned __int8)s1[v16 + 1] + (unsigned __int8)s1[v16 + 2] - 5328;
    v13 = v17 % 26;
    v17 /= 26;
    s1[v29] = v17 / 100 + 48;
    v28[1] = v17 % 100 / 10 + 48;
    v28[2] = v17 % 10 + 48;
  }
  sprintf(&src, "%c", v13 + 97);
  puts(&src);
  strcat(&v35, &src);
  if ( !memcmp(s1, &s2, n) )
    break;
  v13 = 0;
  v14 = 0;
}
strcpy(&buf, &v35);
v18 = strlen(&buf);
```


首先将输入的字符转化为三位十进制数

比如aaa就变成
097097097

然后下面有两个循环，里面那个循环其实就是某种意义上实现一个大数除法

把代码复制下来，跑下看下，我用的是aaa

097097097
003734503
000143634
000005524
000000212
000000008
000000000

其实就是把一个大数除以26，然后把最后三位单独拿出来，余26再加上97，最后拼接起来和hhxptgdlffojwztpewc比较

下面是一个简单的代码，可以把大数给复原

```
b=0
a='hhxptgdlffojwztpewc'
for i in range(len(a)):
    b*=26
    b+=ord(a[len(a)-i-1])-97
    print(b)
```

然后前面补个0，再每三位解析成一个字符就可以了