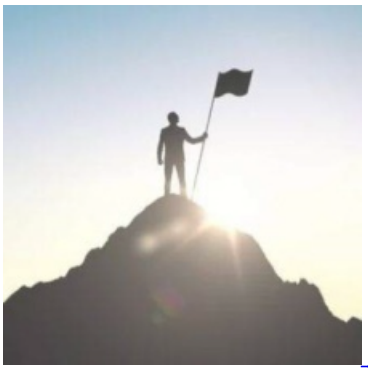
XCTF 进阶 RE zorropub

原创

A_dmins 于 2019-09-28 20:52:07 发布 482 收藏 1

分类专栏： CTF题 XCTF

本文链接：https://blog.csdn.net/qq_42967398/article/details/101636602



XCTF 进阶 RE zorropub

好久没接触CTF了，今天做了一下XCTF中的逆向

有几道题比较简单就不记录了，记录一下这个有点收获的题目吧

首先，我们下载文件，用ida（64）打开看看，找到主函数：

```
int __fastcall main(__int64 a1, char **a2, char **a3)
{
  size_t v3; // rax
  int v5; // [rsp+1Ch] [rbp-104h]
  int v6; // [rsp+20h] [rbp-100h]
  int i; // [rsp+24h] [rbp-FCh]
  unsigned int seed; // [rsp+28h] [rbp-F8h]
  unsigned int v9; // [rsp+2Ch] [rbp-F4h]
  char v10; // [rsp+30h] [rbp-F0h]
  char v11[16]; // [rsp+90h] [rbp-90h]
  char v12[32]; // [rsp+A0h] [rbp-80h]
  char s; // [rsp+C0h] [rbp-60h]
  char s1[40]; // [rsp+E0h] [rbp-40h]
  unsigned __int64 v15; // [rsp+108h] [rbp-18h]

  v15 = __readfsqword(0x28u);
  seed = 0;
  puts("Welcome to Pub Zorro!!");
  printf("Straight to the point. How many drinks you want?", a2);
  __isoc99_scanf("%d", &v5);
  if ( v5 <= 0 )
```

```
{
  printf("You are too drunk!! Get Out!!", &v5);
  exit(-1);
}
printf("OK. I need details of all the drinks. Give me %d drink ids:", (unsigned int)v5);
for ( i = 0; i < v5; ++i )
{
  __isoc99_scanf("%d", &v6);
  if ( v6 <= 16 || v6 > 0xFFFF )
  {
    puts("Invalid Drink Id.");
    printf("Get Out!!", &v6);
    exit(-1);
  }
  seed ^= v6;
}
i = seed;
v9 = 0;
while ( i )
{
  ++v9;
  i &= i - 1;
}
if ( v9 != 10 )
{
  puts("Looks like its a dangerous combination of drinks right there.");
  puts("Get Out, you will get yourself killed");
  exit(-1);
}
srand(seed);
MD5_Init(&v10);
for ( i = 0; i <= 29; ++i )
{
  v9 = rand() % 1000;
  sprintf(&s, "%d", v9);
  v3 = strlen(&s);
  MD5_Update(&v10, &s, v3);
  v12[i] = v9 ^ LOBYTE(dword_6020C0[i]);
}
v12[i] = 0;
MD5_Final((__int64)v11, (__int64)&v10);
for ( i = 0; i <= 15; ++i )
  sprintf(&s1[2 * i], "%02x", (unsigned __int8)v11[i]);
if ( strcmp(s1, "5eba99aff105c9ff6a1a913e343fec67") )
{
  puts("Try different mix, This mix is too sloppy");
  exit(-1);
}
return printf("\nYou choose right mix and here is your reward: The flag is nullcon{%s}\n", v12);
}
```

OK，它的主体意思打开都能看懂，理解起来不难
就是，从上往下走，根据英语的句子也能猜出来大体流程
大意是让我们输两次数，而且我们输入的数与随机数的种子有关
而且还有MD5加密之类的，我们首先能想到的就是爆破，实际上就是爆破
因为是随机的，所以我们需要有一个数组，来进行存放可能的数
可以用python进行编写：

```
a = []

for i in range(16,0xffff):
 c = 0
 j = i
 while(j):
  c = c + 1
  j = j & (j - 1)
 if(c == 10):
  a.append(i)
```

这上面的代码与下面主函数中的代码所对应：

```
  }
  printf("OK. I need details of all the drinks. Give me %d drink ids:", (unsigned int)v5);
for ( i = 0; i < v5; ++i )
{
  __isoc99_scanf("%d", &v6);
  if ( v6 <= 16 || v6 > 0xFFFF )
  {
    puts("Invalid Drink Id.");
    printf("Get Out!!", &v6);
    exit(-1);
  }
  seed ^= v6;
}
i = seed;
v9 = 0;
while ( i )
{
  ++v9;
  i &= i - 1;
}
if ( v9 != 10 )
{
  puts("Looks like its a dangerous combination of drinks right there.");
  puts("Get Out, you will get yourself killed");
  exit(-1);
}
srand(seed);
MD5_Init(&v10);
for ( i = 0; i <= 29; ++i )
```


那么问题就来了，我们如何将我们的数输入到程序中呢？？？

说实话我也是第一次接触这个东西，完全摸不着头脑

看了一下打来的wp才知道，原来可以利用python的一个模块：subprocess

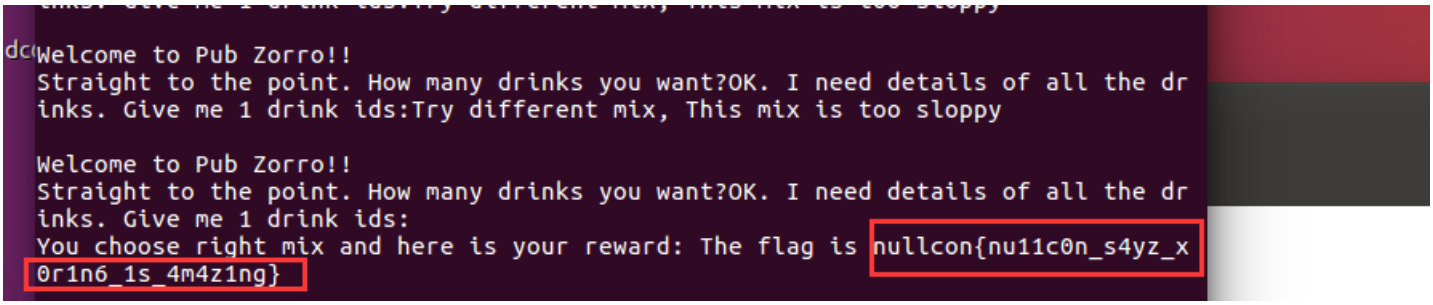
关于这个模块可以看看这个，python subprocess模块使用总结

知道了这个模块如何使用，那么我们就可以进行操作了

编写如下python脚本：

```
import subprocess

a = []

for i in range(16,0xffff):
 c = 0
 j = i
 while(j):
  c = c + 1
  j = j & (j - 1)
 if(c == 10):
  a.append(i)

flag = ""

for i in a:
 proc = subprocess.Popen(['./zorro_bin'], stdin=subprocess.PIPE, stdout=subprocess.PIPE);
 out = proc.communicate(('1\n%s\n'%i).encode('utf-8'))[0]
 #print(out)
 if "nullcon".encode('utf-8') in out:
  print(out)
  break;
```

上部分呢，就是生成字典，下面就是创建一个进程
然后输入两个数据，最后将得到的结果进行返回
再用if来判断返回结果是否包含我们需要的数据，，，
这个题学到的大概就是当我们需要往程序中输入大量数据时
可以利用python来替我们完成这份工作，简直不要太快乐
附上结果：



（PS：别在kali Linux虚拟机上运行，否则会报一个libc错误，不知道是不是我kali的原因咯）