xctf hackme

原创

菜逼的ctf之路 于 2020-10-16 10:34:16 发布 191 收藏 1

xctf hackme

linux执行文件，话不多说直接ida

找到main函数，不会的先查字符串，然后找函数，这个就不教了。

看图

```
_BOOL4 v19; // [rsp+B8h] [rbp-8h]
int i; // [rsp+BCh] [rbp-4h]

sub_407470((__int64)"Give me the password: ", argv, envp, argv);
sub_4075A0((__int64)"%s", v9);
for ( i = 0; v9[i]; ++i )
  ;
v19 = i == 22;
v18 = 10;
do
{
  v7 = sub_406D90((__int64)"%s", (__int64)v9, v3, v4, v5, v6);
  v4 = (unsigned int)(v7 % 22);
  v15 = v7 % 22;
  v17 = 0;
  v14 = byte_6B4270[v7 % 22];
  v13 = v9[v7 % 22];
  v12 = v7 % 22 + 1;
  v16 = 0;
  while ( v16 < v12 )
  {
    ++v16;
    v17 = 1828812941 * v17 + 12345;
  }
  v3 = v17;
  v11 = v17 ^ v13;
  if ( v14 != ((unsigned __int8)v17 ^ v13) )
    v19 = 0;
  --v18;
}
while ( v18 );
if ( v19 )
  v10 = sub_407470((__int64)"Congras\n");
else
```


主要逻辑就是在循环里，这个代码逻辑还是比较简单的，循环找v17，

然后异或，我刚开始也认为很简单，但是有小细节要注意，

注意 注意 注意 重要的事说三遍

看v13的数据类型，是一字节，v17是四字节类型，之后的结果要&0xff，（这个我开始也忘了，导致得不到结果，看了其他大佬的wp才明白）

最后贴上自己的wp

```
a = [
    0x5F, 0xF2, 0x5E, 0x8B, 0x4E, 0x0E, 0xA3,
    0xAA, 0xC7, 0x93, 0x81, 0x3D, 0x5F, 0x74, 0xA3, 0x09,
    0x91, 0x2B, 0x49, 0x28, 0x93, 0x67
]

s=''
for i in range(len(a)):
    j=0
    text=0
    while(j<i+1):
        text=1828812941*text+12345
        j=j+1
    s+=chr(a[i]^text&0x88)
    print(s)
print(s)
```