

逆向-攻防世界-The Maya

转载

自我修炼的小石头 于 2019-05-14 23:47:00 发布 74 收藏

原文链接: <http://www.cnblogs.com/whitehawk/p/10865417.html>

版权

又学会了IDA的新操作。。。

IDA远程调试，可得知获取当前时间。

```
0000559735014A6A mov     rax, [rbp+tp]
0000559735014A6E lea    rax, [rbp+s]
0000559735014A75 mov     rcx, rdx ; tp
0000559735014A78 lea    rdx, aAbcdefghijklmn+40h ; format
0000559735014A7F mov     esi, 63h ; 'c' ; maxsize
0000559735014A84 mov     rdi, rax ; s
0000559735014A87 call   _strftime
0000559735014A8C lea    rax, [rbp+s]
0000559735014A93 mov     rdi, rax
0000559735014A96 call   _strlen
0000559735014A9B mov     [rbp+var_20]

[rbp+s]=[[stack]:00007FFC75375160]
db 32h ; 2
db 30h ; 0
db 31h ; 1
db 39h ; 9
db 2Dh ; -
db 30h ; 0
db 35h ; 5
db 2Dh ; -
db 31h ; 1
db 34h ; 4
```

此处是MD5加密的值

```
0000559735014CAB lea    rax, [rbp+src]
0000559735014CB2 mov     rdi, rax ; s
0000559735014CB5 call   _strlen
0000559735014CBA mov     rbx, rax
0000559735014CBD lea    rax, [rbp+var_120]
0000559735014CC4 mov     rdi, rax ; s
0000559735014CC7 call   _strlen
0000559735014CCC add     rax, rbx
0000559735014CCF add     rax, 1
0000559735014CD3 mov     rdi, rax ; size
0000559735014CD6 call   _malloc
0000559735014CDB mov     [rbp+dest], rax
```

验证正是当前时间MD5加密后的值。

要加密的字符串: 2019-05-14

加密

字符串	2019-05-14
16位 小写	493566263266f695
16位 大写	493566263266F695
32位 小写	ac46447f493566263266f6955958bc2d

然后在这个函数处总是返回null，无法进行继续调试。看了网上的writeup也没明说，都是讲了Maya的日历。卡到这儿了。

```
*dest = 0;
strcat(dest, &md5);
strcat(dest, v11);
v21 = (char *)sub_5597350148A4(dest, v11);
if ( !v21 )
```

今天很晚了，明天就一节课，要把这个操作逆出来。

转载于:<https://www.cnblogs.com/whitehawk/p/10865417.html>