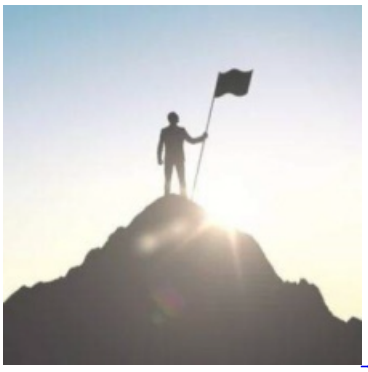
XCTF 进阶 RE APK-逆向2

原创

A_dmins 于 2019-10-01 17:06:47 发布 814 收藏 1

分类专栏： CTF题 XCTF

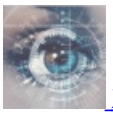
本文链接：https://blog.csdn.net/qq_42967398/article/details/101850382



CTF题 同时被 2 个专栏收录

115 篇文章 11 订阅

订阅专栏



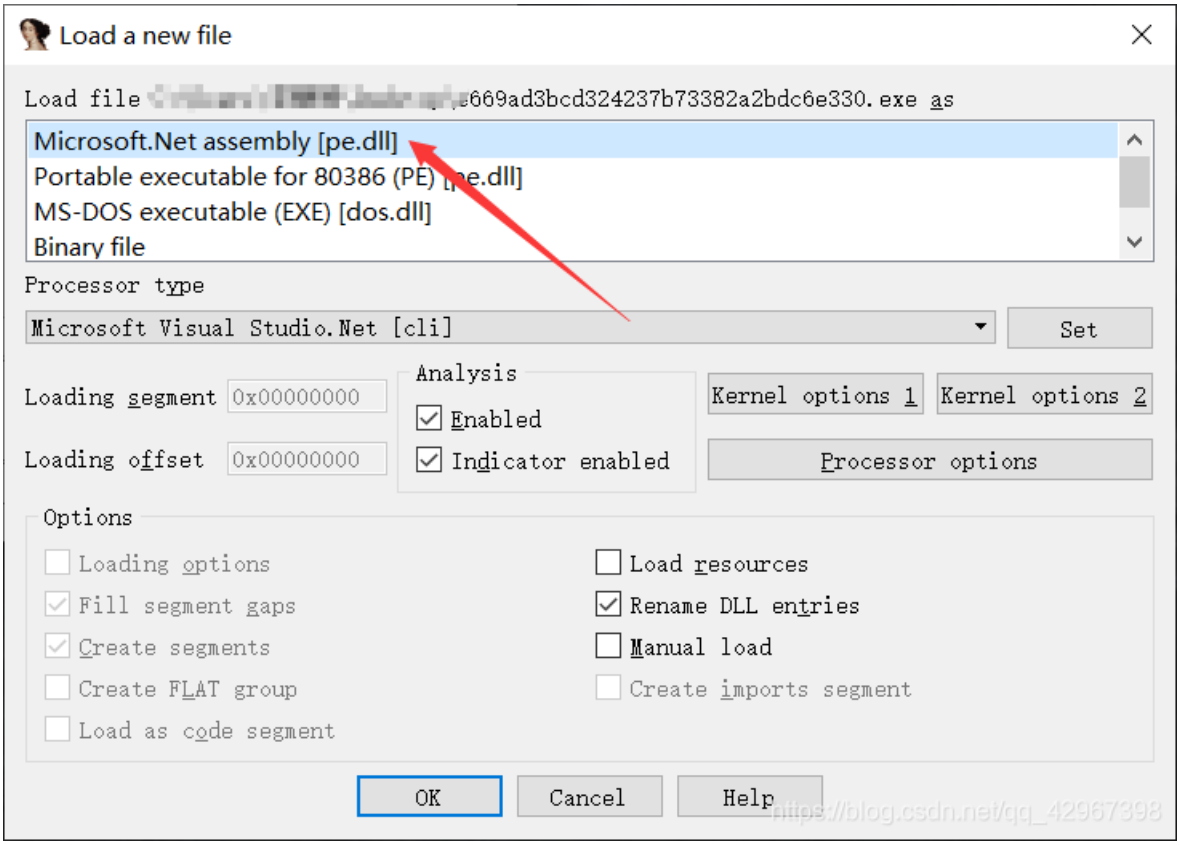
XCTF

24 篇文章 0 订阅

订阅专栏

XCTF 进阶 RE APK-逆向2

要抓紧学习了，感觉要跟不上大佬的步伐了，，，，，
马上要湖湘杯了，不能托大佬后腿，emmm，加油
看题目一开始还以为是安卓的逆向呢，结果不是，，，，
下载文件用ida打开，发现是.net写的，，，



使用ida打开，但是不能编译，所以使用.net的反编译工具，，，dnSpy，，，直接看见源码：

```
using System;
using System.Diagnostics;
using System.IO;
using System.Net.Sockets;
using System.Text;

namespace Rev_100
{
 // Token: 0x02000002 RID: 2
 internal class Program
 {
  // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
  private static void Main(string[] args)
  {
   string hostname = "127.0.0.1";
   int port = 31337;
   TcpClient tcpClient = new TcpClient();
   try
   {
    Console.WriteLine("Connecting...");
    tcpClient.Connect(hostname, port);
   }
   catch (Exception)
   {
    Console.WriteLine("Cannot connect!\nFail!");
    return;
   }
```

```
  Socket client = tcpClient.Client;
  string text = "Super Secret Key";
  string text2 = Program.read();
  client.Send(Encoding.ASCII.GetBytes("CTF{"));
  foreach (char x in text)
  {
   client.Send(Encoding.ASCII.GetBytes(Program.search(x, text2)));
  }
  client.Send(Encoding.ASCII.GetBytes("}"));
  client.Close();
  tcpClient.Close();
  Console.WriteLine("Success!");
 }

 // Token: 0x06000002 RID: 2 RVA: 0x0000213C File Offset: 0x0000033C
 private static string read()
 {
  string fileName = Process.GetCurrentProcess().MainModule.FileName;
  string[] array = fileName.Split(new char[]
  {
   '\\'
  });
  string path = array[array.Length - 1];
  string result = "";
  using (StreamReader streamReader = new StreamReader(path))
  {
   result = streamReader.ReadToEnd();
  }
  return result;
 }

 // Token: 0x06000003 RID: 3 RVA: 0x000021B0 File Offset: 0x000003B0
 private static string search(char x, string text)
 {
  int length = text.Length;
  for (int i = 0; i < length; i++)
  {
   if (x == text[i])
   {
    int value = i * 1337 % 256;
    return Convert.ToString(value, 16).PadLeft(2, '0');
   }
  }
  return "??";
 }
}
}
```

发现就只有三个函数，，，Main()，，，read()，，，search()
整体看上去大概意思就是进行连接，连接上之后发送一串字符串
要求我们求的应该就是这个字符串了，，，，
逐个分析一下函数，，，，其实没学过.net语言，只能靠自己感觉分析一通
Main()函数：

```
    }
    catch (Exception)
    {
        Console.WriteLine("Cannot connect!\nFail!");
        return;
    }
    Socket client = tcpClient.Client;
    string text = "Super Secret Key";
    string text2 = Program.read();
    client.Send(Encoding.ASCII.GetBytes("CTF{"));
    foreach (char x in text)
    {
        client.Send(Encoding.ASCII.GetBytes(Program.search(x, text2)));
    }
    client.Send(Encoding.ASCII.GetBytes("}"));
    client.Close();
    tcpClient.Close();
    Console.WriteLine("Success!");
}
```

调用了read()函数

调用了search()函数

read()函数：

```
private static string read()
{
    string fileName = Process.GetCurrentProcess().MainModule.FileName;
    string[] array = fileName.Split(new char[]
    {
        '\\'
    });
    string path = array[array.Length - 1];
    string result = "";
    using (StreamReader streamReader = new StreamReader(path))
    {
        result = streamReader.ReadToEnd();
    }
    return result;
}
```

获取当前模块的绝对路径

应该是读取文件中的内容，然后return

search()函数：

```
    // Token: 0x06000003 RID: 3 RVA: 0x000021B0 File Offset: 0x000003B0
    private static string search(char x, string text)
    {
        int length = text.Length;
        for (int i = 0; i < length; i++)
        {
            if (x == text[i])
            {
                int value = i * 1337 % 256;
                return Convert.ToString(value, 16).PadLeft(2, '0');
            }
        }
        return "??";
    }
}
```

在text中查找x,找到则将下标进行一系列操作

转为16进制吧，然后不足两位补0

该题大体意思我们应该都清楚了，就是要求我们找到那个字符串，，，

接下来就是根据意思来进行编写python脚本咯

```
# coding=gbk
text='Super Secret Key'

text2 = open('C:\\xxx\\xxx\\xxx\\e669ad3bcd324237b73382a2bdc6e330.exe','r',encoding = 'unicode-escape').read()

flag = "CTF{"
num = len(text2)
def search(i,text2,num):
 for j in range(0,num):
  if i == text2[j]:
   x = j * 1337 % 256
   return '%02x' % x

for i in text:
 flag += search(i,text2,num)

print(flag + '}')
```

得到结果：

```
[redacted]python 1.py
CTF{7eb67b0bb4427e0b43b40b6042670b55}
```

嗯嗯，提交正确，，，，
emmmm，看了wp后，好像还有一个更简单的方法
直接使用python开启服务：

```
import http.server

server_address = ('127.0.0.1', 31337)
handler_class = http.server.BaseHTTPRequestHandler
httpd = http.server.HTTPServer(server_address, handler_class)
httpd.serve_forever()
```

直接就能得到flag，那我还逆向个锤子哦！！！！

```
[redacted]python 1.py
127.0.0.1 - - [01/Oct/2019 17:00:47] code 400, message Bad request syntax ('CTF{7eb67b0bb4427e0b43b40b6042670b55}')
127.0.0.1 - - [01/Oct/2019 17:00:47] "CTF{7eb67b0bb4427e0b43b40b6042670b55}" 400 -
```