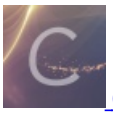
新疆首届安全知识技能大赛writeup

原创

R1ght0us 于 2018-09-17 19:17:57 发布 1109 收藏

分类专栏： CTF 文章标签： MISC CTF比赛

本文链接：https://blog.csdn.net/qq_39495209/article/details/82747475



总是把比赛想的太简单，原来在哪里总是藏龙卧虎，不能小瞧任何人，也别高看了自己。但是这是第一次参加**不让联网**的CTF比赛！

> stay foolish,stay hungry

如来十三掌

通过这个题目，让我联想到与佛论禅和rot13加密，那么打开题目，下载下来一个docx文档。下面加粗的文字即是打开文档的内容。

夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三佧三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤磔他哆提哆多缽以南哆心曰姪罰蒙吶神。舍切真怯勝吶得俱沙罰娑是怯遠得吶數罰輪哆遠薩得槃漫夢盧皤亦醯吶娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮

首先我们打开与佛论禅，在其加密内容前加上**佛曰：**。如图所下：

下面是这个解出来密文，显然还有一层加密。

```
MzkuM3gvMUAwnzuvn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9
```

猜测~~base64~~编码，结果没有解出来。联系题目猜测为rot13加密

解码出来继续base64解码，在此之后我会写相关的加密的详解。

取证内存镜像flag

这道题给了hint才知道是内存取证，但是因为自己起初没在意相关工具的使用~~其实就是自己懒~~，那么这次的惨败正好弥补自己的不足。

volatility是专门进行内存取证的工具，对于windows系统比较友好，linux系统需要单独的安装相应的插件。

```
-f  选择所要取证的镜像文件```
进行镜像识别
```text
imageinfo
```

我们可以发现volatility建议我们使用**WinXPSP2x86**，那么继续使用查看当时的dump下来的内存中存在的进程

```
--profile  使用哪一种镜像进行取证
```

```
pslist  查看当时dump下来所运行的进程
```

然而根据题目，我们猜测应该在是某个文件，那么扫描目录，其中为了查询相关字符，进行了管道命令以及`grep`进行筛选。

```
filescan  文件扫描
```

那么下面我就进行导出其相关文件。

```
dumpfiles 导出文件
```

```
-Q   所要导出文件的地址
```

```
--dump-dir  导出文件所要存在那个目录里
```


打开发现这个压缩包需要密码，我猜测了许多种可能，密码应该在剪切板中，于是搜索剪切板的内容

```
clipboard    查看剪切板的内容
```

于是尝试是否这个剪切板的内容就是密码，获得flag

> 这个是**真·取证**，让我感觉到这个CTF还是能够提高我在安全的其他方面的。

流量包解密02

果然还是见识少，所有的比赛的束手无措只是自己平时懒所付出的代价。
下载下来一看，文件是`.cap`结尾的格式，那么应该是WiFi所抓下来的包，而且题目提示密码就是本机的MAC地址。那么我们需要用到**aircrack-ng**工具解密流量。
```

先用wireshark打开流量包可以看到我们MAC地址（无线>wlan流量）

aircrack-ng解密流量，有个坑**密码MAC地址大写**

```
-w    使用密码字典
```

然后将key值导入进去(**首选项>protpcols>IEEE 802.11>Decryption key>wpa-key**)

然后追踪TCP流

最后查看网址找到了flag

Referer

https://blog.csdn.net/qq_28208251/article/details/48093575
https://xz.aliyun.com/t/1972
http://netsecurity.51cto.com/art/201105/264844.htm
https://blog.csdn.net/dmbjzhh/article/details/79425483

> **如果有同学需要上述题目，请联系我**