10

发表于 2021-08-30 分类于 Challenge， 2021， 工业信息安全技能大赛， 巡回赛-兰州站
Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-兰州站 | 10

点击此处获得更好的阅读体验

WriteUp来源

来自M01N战队

题目描述

> *数据包为某黑客入侵后留下的证据，黑客疑似使用DNS相关操作将窃取的信息传输了出去，请找出黑客传输的信息内容。*

题目考点

- *DNS协议*
- *Shellcode调试*

解题思路

提取DNS PTR查询的响应内容（共23个），为十六进制编码

```
d9eb9bd97424f431d2b27731c9648b
71308b760c8b761c8b46088b7e208b
36384f1875f35901d1ffe1608b6c24
248b453c8b54287801ea8b4a188b5a
2001ebe334498b348b01ee31ff31c0
fcac84c07407c1cf0d01c7ebf43b7c
242875e18b5a2401eb668b0c4b8b5a
1c01eb8b048b01e88944241c61c3b2
0829d489e589c2688e4e0eec52e89f
ffffff894504bb7ed8e273871c2452
e88effffff894508686c6c20416833
322e64687573657230db885c240a89
e656ff550489c250bba8a24dbc871c
2452e85fffffff6861677d58686465
666c685f6a6961685f736869687b7a
686568666c616731db885c241589e3
6858202020684d545239684d545131
6859576b786859573973685a53316b
68626d6c6b68626d6374684c586c70
6864574675685a69316f6864574e30
685957357a685a33746e685a6d7868
31c9884c243889e131d252535152ff
d031c050ff5508
```

shellcode代码，运行即可：

base64 解密得到flag

Flag

```
flag{gansuctf-huan-ying-nide-daolai114514}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/巡回赛-兰州站/tZqo4dzcJnKDMkJgcNK8xQ.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2021 # 工业信息安全技能大赛 # 巡回赛-兰州站
2
09