10

2021-08-30 | 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

```
0.1.1.1.in-addr.arpa: type PTR, class IN, "d9eb9bd97424f431d2b27731c9648b
1.1.1.1.in-addr.arpa: type PTR, class IN, "71308b760c8b761c8b46088b7e208b
2.1.1.1.in-addr.arpa: type PTR, class IN, "36384f1875f35901d1ffe1608b6c24
3.1.1.1.in-addr.arpa: type PTR, class IN, "248b453c8b54287801ea8b4a188b5a
4.1.1.1.in-addr.arpa: type PTR, class IN, "2001ebe334498b348b01ee31ff31c0
5.1.1.1.in-addr.arpa: type PTR, class IN, "fcac84c07407c1cf0d01c7ebf43b7c
6.1.1.1.in-addr.arpa: type PTR, class IN, "242875e18b5a2401eb668b0c4b8b5a
7.1.1.1.in-addr.arpa: type PTR, class IN, "1c01eb8b048b01e88944241c61c3b2
8.1.1.1.in-addr.arpa: type PTR, class IN, "0829d489e589c2688e4e0eec52e89f
9.1.1.1.in-addr.arpa: type PTR, class IN, "ffffff894504bb7ed8e273871c2452
10.1.1.1.in-addr.arpa: type PTR, class IN, "e88effffff894508686c6c20416833
11.1.1.1.in-addr.arpa: type PTR, class IN, "322e64687573657230db885c240a89
12.1.1.1.in-addr.arpa: type PTR, class IN, "e656ff550489c250bba8a24dbc871c
13.1.1.1.in-addr.arpa: type PTR, class IN, "2452e85fffffff6861677d58686465
14.1.1.1.in-addr.arpa: type PTR, class IN, "666c685f6a6961685f736869687b7a
15.1.1.1.in-addr.arpa: type PTR, class IN, "686568666c616731db885c241589e3
16.1.1.1.in-addr.arpa: type PTR, class IN, "6858202020684d545239684d545131
17.1.1.1.in-addr.arpa: type PTR, class IN, "6859576b786859573973685a53316b
18.1.1.1.in-addr.arpa: type PTR, class IN, "68626d6c6b68626d6374684c586c70
19.1.1.1.in-addr.arpa: type PTR, class IN, "6864574675685a69316f6864574e30
20.1.1.1.in-addr.arpa: type PTR, class IN, "685957357a685a33746e685a6d7868
21.1.1.1.in-addr.arpa: type PTR, class IN, "31c9884c243889e131d252535152ff
22.1.1.1.in-addr.arpa: type PTR, class IN, "d031c050ff5508
```

```
1  d9eb9bd97424f431d2b27731c9648b
2  71308b760c8b761c8b46088b7e208b
3  36384f1875f35901d1ffe1608b6c24
4  248b453c8b54287801ea8b4a188b5a
5  2001ebe334498b348b01ee31ff31c0
6  fcac84c07407c1cf0d01c7ebf43b7c
7  242875e18b5a2401eb668b0c4b8b5a
8  1c01eb8b048b01e88944241c61c3b2
9  0829d489e589c2688e4e0eec52e89f
10 ffffff894504bb7ed8e273871c2452
11 e88effffff894508686c6c20416833
12 322e64687573657230db885c240a89
13 e656ff550489c250bba8a24dbc871c
14 2452e85fffffff6861677d58686465
15 666c685f6a6961685f736869687b7a
16 686568666c616731db885c241589e3
17 6858202020684d545239684d545131
18 6859576b786859573973685a53316b
19 68626d6c6b68626d6374684c586c70
20 6864574675685a69316f6864574e30
21 685957357a685a33746e685a6d7868
```

```
31c9884c243889e131d252535152ff
d031c050ff5508
```

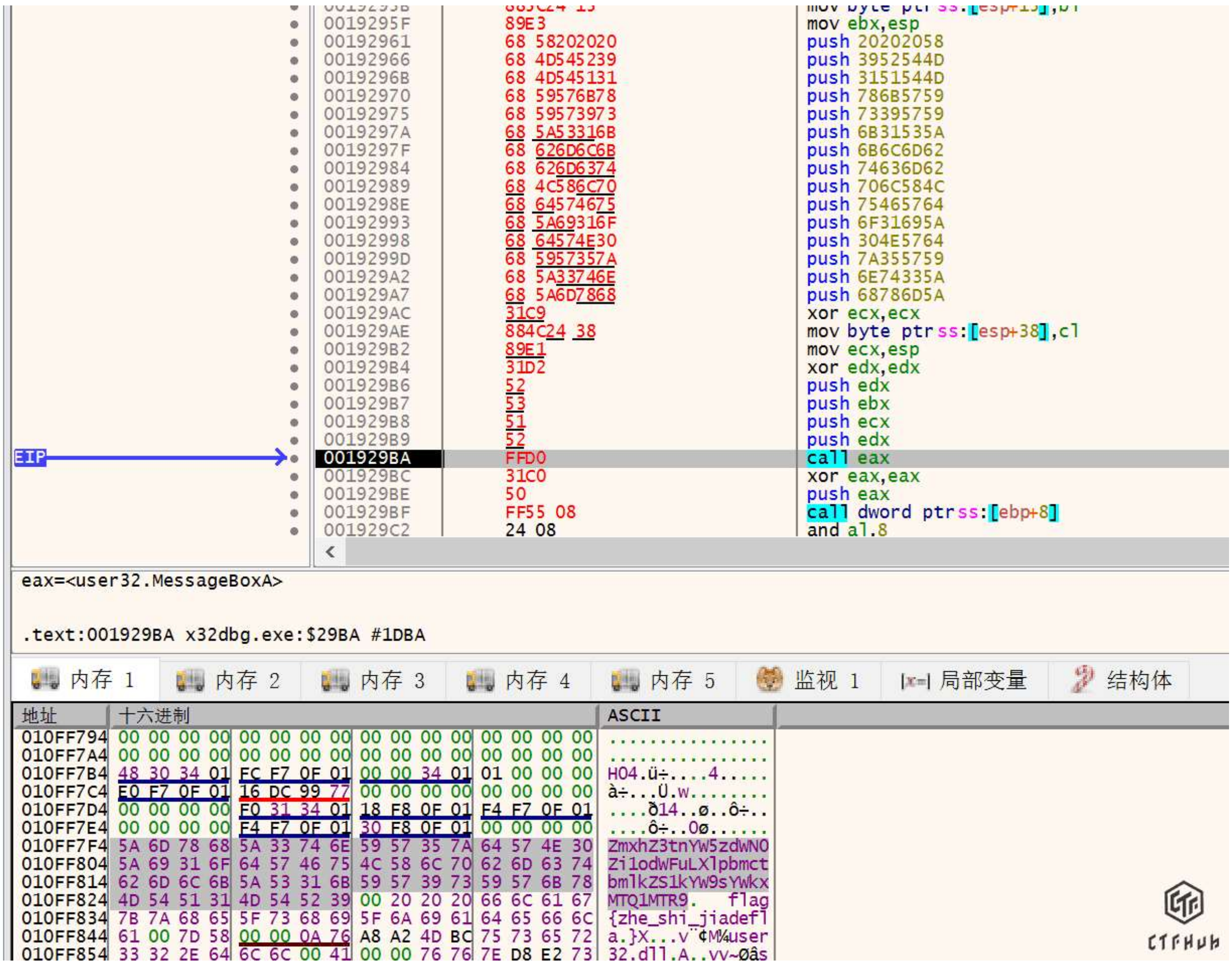
```
666c685f6a6961685f736869687b7a
686568666c616731db885c241589e3
6858202020684d545239684d545131
6859576b786859573973685a53316b
68626d6c6b68626d6374684c586c70
6864574675685a69316f6864574e30
685957357a685a33746e685a6d7868
31c9884c243889e131d252535152ff
d031c050ff5508
```

16进制转字符 字符转16进制 测试用例 清空结果 复制结果

```
,麓Xw1ɤ夥旹蝍O•u遑朂$5ڬx•ℵ•  4IZ㸶4•O
•ọ噛(uH̦$•룟•K  •鄳•aò•)ル剂h刢  •/•$R莿刨ll Ah32.dhuser0ʒ\$
  喍M笑_衦}Xhdeflh_jiah_shih{zhehflag1ʒ\$•靈 hMTR9hMTQ1hYWkxhYW9shZS1khbmlkhbmcthLXlphdWFuhZi1ohdWN0hYW5zhZ3tnhZmxh1JL$812.QRnU•
```

shellcode代码，运行即可：

88



base64 解密得到flag

Flag

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


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

2 09