



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, "ffffffff894504bb7ed8e273871c2452
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, "2452e85fffffffff6861677d58686465
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 fffffffff894504bb7ed8e273871c2452
11 e88effffff894508686c6c20416833
12 322e64687573657230db885c240a89
13 e656ff550489c250bba8a24dbc871c
14 2452e85fffffffff6861677d58686465
15 666c685f6a6961685f736869687b7a
16 686568666c616731db885c241589e3
17 6858202020684d545239684d545131
18 6859576b786859573973685a53316b
19 68626d6c6b68626d6374684c586c70
20 6864574675685a69316f6864574e30
21 685957357a685a33746e685a6d7868
```

2231c9884c243889e131d252535152ff

23d031c050ff5508

15666c685f6a6961685f736869687b7a

16686568666c616731db885c241589e3

176858202020684d545239684d545131

186859576b786859573973685a53316b

1968626d6c6b68626d6374684c586c70

206864574675685a69316f6864574e30

21685957357a685a33746e685a6d7868

2231c9884c243889e131d252535152ff

23d031c050ff5508

16进制转字符

字符转16进制

测试用例

清空结果

复制结果

1, 玆Xw1x豉告判O•u遑豉\$豉x*• 4Iz豉4•O

2•q叫(uH,\$•豉•K •豉•a•)•u剂h豉 •/•\$R荆创II Ah32.dhuser0j\,\$

3 豉M英_衬)Xhdeflh_jiah_shih{zhehflag}j\,\$•豉 hMTR9hMTQ1hYwKxhYW9shZS1kxhbm1kxhbmcthlXlphdWFuhZi1ohdWN0hYW5zhZ3tnhZmxh1JL\$812.QRnU•

shellcode代码，运行即可：

88

• 0019295B 89E3 mov byte ptr [esp+10],0

• 0019295F 68 58202020 push 20202058

• 00192961 68 4D545239 push 3952544D

• 00192966 68 4D545131 push 3151544D

• 0019296B 68 59576B78 push 786B5759

• 00192970 68 59573973 push 73395759

• 00192975 68 5A53316B push 6B31535A

• 0019297A 68 626D6C6B push 6B6C6D62

• 0019297F 68 626D6374 push 74636D62

• 00192984 68 4C586C70 push 706C584C

• 00192989 68 64574675 push 75465764

• 0019298E 68 5A69316F push 6F31695A

• 00192993 68 64574E30 push 304E5764

• 00192998 68 5957357A push 7A355759

• 0019299D 68 5A33746E push 6E74335A

• 001929A2 68 5A6D7868 push 68786D5A

• 001929A7 31C9 xor ecx,ecx

• 001929AC 884C24 38 mov byte ptr ss:[esp+38],c1

• 001929AE 89E3 mov ecx,esp

• 001929B2 31D2 xor edx,edx

• 001929B4 52 push edx

• 001929B6 53 push ebx

• 001929B7 51 push ecx

• 001929B8 52 push edx

• 001929B9 FF00 call eax

• 001929BC 31C0 xor eax,eax

• 001929BE 50 push eax

• 001929BF FF55 08 call dword ptr ss:[ebp+8]

• 001929C2 24 08 and al,8

eax=<user32.MessageBox>

.text:001929BA x32dbg.exe:\$29BA #1DBA

内存 1 内存 2 内存 3 内存 4 内存 5 监视 1 |x=| 局部变量 结构体

地址	十六进制	ASCII
010FF794	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010FF7A4	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
010FF7B4	48 30 34 01 FC F7 0F 01 00 00 34 01 01 00 00 00	H04.ü÷...4.....
010FF7C4	F0 F7 0F 01 16 DC 99 77 00 00 00 00 00 00 00 00	à÷...ü.w.....
010FF7D4	00 00 00 00 F0 31 34 01 18 F8 0F 01 F4 F7 0F 01	...014...0÷... ..
010FF7E4	00 00 00 00 F4 F7 0F 01 30 F8 0F 01 00 00 00 00	...0÷...00.....
010FF7F4	5A 6D 78 68 5A 33 74 6E 59 57 35 7A 64 57 4E 30	ZmxhZ3tnYW5zdWN0
010FF804	5A 69 31 6F 64 57 46 75 4C 58 6C 70 62 6D 63 74	Zi1odwFuLX1pbmct
010FF814	62 6D 6C 68 5A 53 31 68 59 57 39 73 59 57 68 78	bm1kZS1kYw9sYkx
010FF824	4D 54 51 31 4D 54 52 39 00 20 20 20 66 6C 61 67	MTQ1MTR9. flag
010FF834	78 7A 68 65 5F 73 68 69 5F 6A 69 61 64 65 66 6C	{zhe_shi_jiadeFl
010FF844	61 00 7D 58 00 00 0A 76 A8 A2 4D BC 75 73 65 72	a.}X...V 4M4user
010FF854	33 32 2E 64 6C 6C 00 41 00 00 76 76 7E D8 E2 73	32.d11.A...vv-oas

base64 解密得到flag

Flag



```
1 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 >

© 2019 – 2022 ❤ CTFHub

由 [Hexo](#) & [NexT.Gemini](#) 强力驱动