Stefano / 2018-10-31 06:52:00 / 浏览数 3260 安全技术 CTF 顶(0) 踩(0)

前言

本篇是Forensic,即取证类的题解。包括有一些常规的入门misc题目,比如流量分析,图片、文件隐写之类的。部分题目附件已打包。链接: https://pan.baidu.com/s/lkfx8GEnio7V1Z5Fa4TrfMQ 提取码: 5a9u

(拖了半个月终于把这篇补完了,还好题目还开着,拖延症彻底没救了-0-.....)

Forensics Warmup 1

Question

Can you unzip this file for me and retreive the flag?

Hint

Make sure to submit the flag as picoCTF{XXXXX}

Solution

签到题,解压zip,得到flag.jpg



输入图上的字符就行了。

 $flag: \verb|picoCTF{welcone_to_forensics}|$

Forensics Warmup 2

Question

Hmm for some reason I can't open this PNG? Any ideas?

Hint

How do operating systems know what kind of file it is? (It's not just the ending!

Make sure to submit the flag as picoCTF{XXXXX}

Solution

使用file命令查看图片的文件格式。

> file flag.png

flag.png: JPEG image data, JFIF standard 1.01, resolution (DPI), density 75x75, segment length 16, baseline, precision 8, 909>

本质是jpg文件,修改后缀为.jpg就可以打开了。(其实大多的图片浏览器都可以直接打开这种单纯修改一下后缀的图片)

 ${\sf flag:} {\tt picoCTF} \{ {\tt extensions_are_a_lie} \}$

Desrouleaux

Question

Our network administrator is having some trouble handling the tickets for all of of our incidents. Can you help him out by answering all the questions? Connect with no 2018shell1.picocff.com 54782. incidents.json

If you need to code, python has some good libraries for it.

Solution

文件里面是一段json数据。

```
"ticket_id": 0,
    "timestamp": "2015/05/09 22:28:20",
    "file_hash": "b807c12fc3e10ba3",
    "src_ip": "248.63.150.241",
    "dst_ip": "251.0.92.254"
},

{
    "ticket_id": 1,
    "timestamp": "2016/12/27 04:01:52",
    "file_hash": "1698b8b87f51ce8e",
    "src_ip": "248.63.150.241",
    "dst_ip": "116.196.246.151"
},
```

nc到问题服务器,一步步处理后发现有三个问题:

- 1. What is the most common source IP address?
- 2. How many unique destination IP addresses were targeted by the source IP address 236.232.221.165?
- 3. What is the average number of unique destination IP addresses that were sent a file with the same hash? Your answer needs to be correct to 2 decimal places.

第三个有点拗口,大概意思就是要算出每个单独的文件发送到的ip地址个数的平均数是多少。使用python的list和dict对象可以很方便的处理这些数据。

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
import json
import re
from pwn import *
with open('./incidents.json') as f:
  text = f.read()
text = json.loads(text)
r = remote('2018shell2.picoctf.com', 54782)
src_ip_count = {}
dst_ip_count = []
unique_dst_ip = 0
hash_dst_ip = {}
r.recvuntil('common ones.')
for i in text['tickets']:
   # Question 1
   if i['src_ip'] not in src_ip_count.keys():
      src_ip_count[i['src_ip']] = 1
   else:
       src_ip_count[i['src_ip']] += 1
r.sendline(max(src_ip_count))
content = r.recvuntil('?\n')
content = re.findall(r'address \d{1,3}.\d{1,3}.\d{1,3}.\d{1,3} ?',content)
content = ''.join(content).split(' ')[1]
```

```
for i in text['tickets']:
   # Ouestion 2
   if i['dst_ip'] not in dst_ip_count and i['src_ip'] == content:
       dst_ip_count.append(i['dst_ip'])
       unique_dst_ip += 1
   # Question 3
   if i['file_hash'] not in hash_dst_ip.keys() and i['file_hash'] != []:
      hash_dst_ip[i['file_hash']] = []
       hash_dst_ip[i['file_hash']].append(i['dst_ip'])
   elif i['file_hash'] in hash_dst_ip.keys() and i['file_hash'] != []:
       hash_dst_ip[i['file_hash']].append(i['dst_ip'])
avg = 0
for i in hash_dst_ip:
  avg += len(hash_dst_ip[i])
avg = avg * 1.0 / len(hash_dst_ip)
# print unique_dst_ip
# print round(avg, 2)
r.sendline(str(unique_dst_ip))
r.sendline(str(round(avg, 2)))
# r.interactive()
print r.recvuntil('}\n')
r.close()
运行脚本得到flag。
```

flag:picoCTF{J4y_s0n_d3rUUUULo_c74e3495}

Reading Between the Eyes

Question

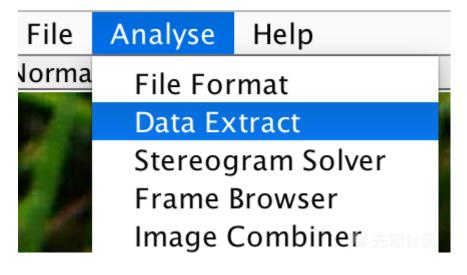
Stego-Saurus hid a message for you in this image, can you retreive it?

Hint

Maybe you can find an online decoder?

Solution

LSB隐写,使用stegsolve提取最低位。



Extract Preview				
7069636f4354467b 72333464316e675f picoCTF{ r34dlng				
62333777333336e5f 3768335f62793733 b37w33n 7h3 by73				
737d0000000000 000000000000000 s}				
000000000000000000000000000000000000000				
000000000000000000000000000000000000000				
00000000000000 000000000000000				
00000000000000 00000000000000				
00000000000000 0000000000000				
00000000000000 0000000000000				
00000000000000 0000000000000				
Bit Planes	☐ Order settings			
Alpha 7 6 5 4 3 2 1 0	Extract By O Row Column			
Red 7 6 5 4 3 2 1 0	Bit Order MSB First LSB First			
Green 7 6 5 4 3 2 1 0	Bit Plane Order			
Blue	ORGB GRB			
	RBG BRG			
Preview Settings	O CRD O DCD			
Include Hex Dump In Preview 🗸	○ GBR ○ BGR			
<u> </u>	<u> </u>			
Preview Save Text Save Bi	in Cancel			

勾选RGB信道的最低位0,顺序是LSB First,就可以看到flag。

 $flag: \verb|picoCTF| \{ r34dlng_b37w33n_7h3_by73s \}$

Recovering From the Snap

Question

There used to be a bunch of <u>animals</u> here, what did Dr. Xernon do to them?

Hint

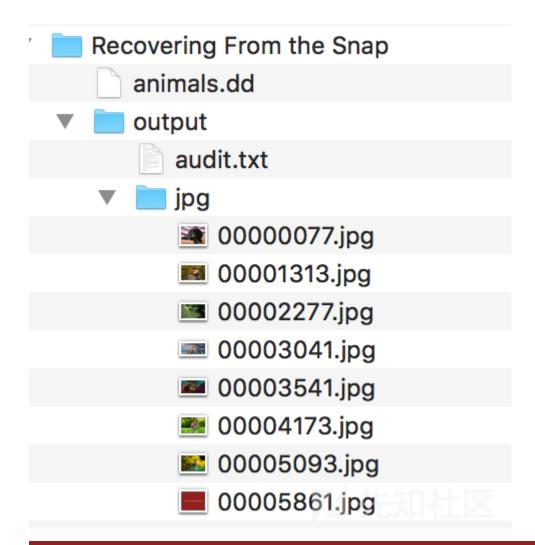
Some files have been deleted from the disk image, but are they really gone?.

Solution

使用binwalk查看文件,发现有很多隐写进去的jpg文件,用foremost提取出来。

> foremost animals.dd
foremost: /usr/local/etc/foremost.conf: No such file or directory
Processing: animals.dd
|*|

提取完成查看图片,可以看到最后一张就是flag。



picoCTF{th3_5n4p_happ3n3d}

▶ 先知社区

flag:picoCTF{th3_5n4p_happ3n3d}

admin panel

Question

We captured some traffic logging into the admin panel, can you find the password?

Hint

Tools like wireshark are pretty good for analyzing pcap files.

Solution

使用wireshrak打开pcap流量包,追踪tcp流,在第5个流可以看到flag。

5	P(8 8	DST /login HTTP/1.1 (a 标记/取消标记 分组(M) 忽略/取消忽略 分组(I)	applicat 器M 器D	tion/x-www- Win=30080 =477 Win=3	Len=0 TS\
1 5 5 5	3 8 3 H	设置/取消设置 时间参考时间平移 分组注释	第T 公 第T 公 第C		2 Len=0 TS 0 Len=1448 128 Len=0
	3	编辑解析的名称		ck=1750 W: 78 Win=300	
	8	作为过滤器应用 准备过滤器 对话过滤器 对话着色 SCTP		YO WIII-JOK	DOU LEII-U
		追踪流	>	TCP 流	T第位了
		复制	>	UDP 流 SSL 流	U 器 位 了
_	_	协议首选项 解码为(A) 在新窗口显示分组(W)	•	HTTP 流	℃分器H

```
POST /login HTTP/1.1
Host: 192.168.3.128
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:59.0) Gecko/20100101 F:
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.3.128/
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Connection: keep-alive
Upgrade-Insecure-Requests: 1

user=admin&password=picoCTF{n0ts3cur3_13597b43}
HTTP/1.0 200 OK
Content-Type: text/ntml; charset=utt-8
```

分组字节流 ❖	宽窄	♦ 区分大小写 正	则表达式	picoCTF{.	*?}
Time	Source	Destination	Protocol	Length	Info
46 14.665168	192.168.3.129	192.168.3.128	TCP	66	37946
47 14.665356	192.168.3.128	192.168.3.129	HTTP	653	HTTP/1
48 14.665366	192.168.3.129	192.168.3.128	TCP	66	37946
49 14.665616	192.168.3.129	192.168.3.128	TCP	66	37946
50 14.665986	192.168.3.128	192.168.3.129	TCP	66	80 → 3
51 14.671005	192.168.3.129	192.168.3.128	TCP	74	37948
52 14.673137	192.168.3.128	192.168.3.129	TCP	74	80 → 3
53 14.673166	192.168.3.129	192.168.3.128	TCP	66	37948
54 14.673355	192.168.3.129	192.168.3.128	HTTP	424	GET /
55 14.673677	192.168.3.128	192.168.3.129	TCP	66	80 → 3
56 14.675242	192.168.3.128	192.168.3.129	TCP	83	80 → 3
57 14.675258	192.168.3.129	192.168.3.128	TCP	66	37948
58 14.675527	192.168.3.128	192.168.3.129	TCP	1514	80 → 3
59 14.675536	192.168.3.129	192.168.3.128	TCP	66	37948
60 14.675592	192.168.3.128	192.168.3.129	HTTP	906	HTTP/1
61 14.675603	192.168.3.129	192.168.3.128	TCP	66	37948
62 14.675660	192.168.3.128	192.168.3.129	TCP	66	80 → 3
63 14.675853	192.168.3.129	192.168.3.128	TCP	66	37948
64 14.676112	192.168.3.128	192.168.3.129	TCP	66	80 → 3
65 37.234094	192.168.3.129	192.168.3.128	TCP	74	38526
66 37.234695	192.168.3.128	192.168.3.129	TCP	74	80 → 3
67 37.234718	192.168.3.129	192.168.3.128	TCP	66	38526
68 37.234879	192.168.3.129	192.168.3.128	HTTP	542	POST /
60 27 225275	10ን 16ዩ ፯ 1ንዩ	10ን 16ዩ ፯ 1ንዐ	TCD	66	QA _ :

[Timestamps]

TCP payload (476 bytes)

ypertext Transfer Protocol TML Form URL Encoded: application/x-www-form-urlencoded 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f Referer : http:/ 2f 31 39 32 2e 31 36 38 2e 33 2e 31 32 38 2f 0d /192.168 .3.128/ 54 79 0a 43 6f 6e 74 65 6e 74 2d 70 65 3a 20 61 ·Content -Type: a 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 pplicati on/x-www 0 6f 72 2d 75 65 6e 63 6f 64 -form-ur lencoded 2d 66 6d 72 6c 65 64 0d 0a 43 6f 6e 74 65 6e 2d 4c 65 6e 67 74 68 ··Conten t-Length 3a 20 35 33 0d 0a 43 6f 6e 6e 65 63 74 69 6f : 53 · Co nnection 3a 20 6b 65 65 70 2d 61 69 76 65 0d 0a 55 70 : keep-a live Up 6c 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 grade-In secure-R 71 75 73 74 73 3a 20 31 0d 0a 75 73 65 65 0a 0d equests: **1** ⋅ ⋅ ⋅ us 64 72 3d 61 6d 69 6e 26 70 61 73 73 77 6f 72 er=admin &passwor 9 3d 70 69 63 6f 43 54 46 7b 6e 30 74 73 33 63 d=picoCT F{n0ts3c 75 72 33 5f 31 33 35 39 37 62 34 33 7d ur3 1359 7b43}

flag:picoCTF{n0ts3cur3_13597b43}

hex editor

Question

This cat has a secret to teach you. You can also find the file in /problems/hex-editor_2_c1a99aee8d919f6e42697662d798f0ff on the shell server.

What is a hex editor?

Maybe google knows.

xxd

hexedit

<u>bvi</u>

Solution

使用16进制编辑器查看文件16进制内容, windows环境下可以使用winhex、010editor, mac环境下可以使用hex friend。

```
hex_editor.jpg
                                                                                         ..A..j... .<..E..Vt.;W.....*...D
75204 00D8AF41 96D56AAB D8AB0AB0 3CEAE345 FEEA5674 BA3B57A7 CDA7AFF7 2A8DC69A B5441E5F
                                                                                        q... g.Y..G.4...J..[=....N.R8...T%j
75240 71A4B2FF 000567DC 59EDAF47 D434F5F9 BE4AE5F5 5B3DBBAB 9EAC4E8A 5238FB85 DB54256A
75276 DBD421DB 58970BB6 B8A513AA 3228CD55 66AB5355 3B86A92C 8256A622 D0ED4D76 A0827493
                                                                                        ..!.X. ... .2(.Uf.SU;..,.V."..Mv..t.
75312 6D1E7553 79BFB94F B75F9F73 55126ADB FCDD6AB6 A7F32559 8BEE5417 ABB92AC0 E6EED6B3
                                                                                        m uSy..O._.sU j...j...%Y..T ..*....
75348 255ADABB 5DB59571 F7AB2901 4DD69952 B5455002 514B4940 05145140 05145140 0B56A26F
                                                                                        %Z..]..q..) M..R.EP QKI@ Q@ V.o
      92AAA2D4 BBAAC095 DBE7A725 4156A1A0 0627DFA2 6FB8284F BF44B401 055CB45F 92A28A3A
                                                                                        ١._..:
                                                                                        .o [I.. r.. .V.$Y"0.{.. U...y0V.l
75420 B96F1D11 035B49AB D77F72A9 D91DA956 AE245922 4FEF7BD6 A4141155 AA9DC379 4F56B76C
75456 7DA6A0BA 8F726EA8 2C81E4DC 955FF8E8 DACAF52E DF928020 9569A9F2 548EBF3D 35D6A407
                                                                                        }....rn.,..._........i..T..=5..
75492 236FA54F BF4C8AA6 A009924F 969BE653 29AED540 4BE66E4A AB70B4E4 6F9E89A8 02045A7E
                                                                                        #o.0.L... .0...S)..@K.nJ.p..o... Z~
75528 DA9225A9 5E3F9680 29EDA6BA D4FB7E7A 1D6802AB AD4753BA D4552036 9D435351 A8024DDB
                                                                                        ..%.^?..)....~z h ..GS..U 6.CSQ. M.
75564 6A589AA0 6A96DFEF 5005E897 755CB55A 6DA47571 23DB5BC6 24487797 55A5564F BB57372D
                                                                                        jX..j...P ..u\.Zm.ug#.[.$Hw.U.VO.W7-
                                                                                        W.mX ..'j&..& . ~.J( .2.e ..s..SwQ..
75600 57976D58 159DAA27 6A26A8AB 2600FF00 7E8A4A28 03F4328A 650ED5D4 738FA653 7751BA80
75636
     1D4DDD4C DD450014 94514005 42ED4FA6 D0031A9B 52D26DA0 08B6D35D 6A775A6E DAB24836
                                                                                         M.L.E .Q@ B.O.. .R.m. ..]jwZn..H6
75672 D33CB5AB 5B699B68 02B3C6B5 56E215AD 175AAB2C 740181A8 5BAD725A C42BB1AB B9BD5F92
                                                                                        .<..[i.h ...V. . Z.,t ..[.rZ.+..._.
75708 B94D6E35 D8D44CA8 9E7DAAC7 F7EB9BBB FBF5D5EB 6BF7AB94 D43E476A E2A875C4 CCB86ACE
                                                                                        .Mn5..L..}......k....>Gj..u...j.
                                                                                        .j.p.Fj.....U.Z.j. .CPnZr6. ..j.=.
... Z._....cP..X. ......&...d M.
75744 B86AB970 D5466AC8 D481DAAB BB55875A 8B6AD003 16AD4350 6E5A7236 FA0891A3 6AD53DDA
75780 FC95169F 1D5ABB5F 92B78994 8E6350FB ED58B70D F3D6DEA5 F7DEB126 FBE2B299 640D4DA1
75816 E9959005 25145001 45145001 4B494500 49BA8A62 D3EAC072 2D5A45F9 2A2B75AB 28B4011D
                                                                                        ... % P E P KIE I..b...r-ZE.*+u.(.
75852 31EAD797 F2D40EB4 013DAAD6 8C50FCF5 9768DB1E B76C997E 5AD22412 A47B52A2 DDFC1571
                                                                                        1..... = ...P...h. .1.~Z.$ .{R... q
75888 E45F9EA9 BAFC95A3 01AF1FCF 52A43F25 0F8F969C 922D4019 D776FB5E 848D592A 5BE92A04
                                                                                          _..... . .R.?% ....-@ .v.^..Y*[.*
75924 91552802 2B85DAFF 002D559A AD4B26EA AAFF0072 A0B1A9F7 E9C8D494 89F7EA40 B891EEA6
                                                                                        .U( +... -U..K&... r.....@....
75960 CB1FC953 DA7DCA96 E23F92AB 940C94F9 5E9CD4F7 5F9E99B6 8008BEFD 5A6AAAB5 61EAC822
                                                                                        . .S.}...?... ..^..._... ..Zj..a.."
75996 7FBF4C6A 7BD3256A 802B4AD5 153A5A6A D49639D7 E4A83857 AB88BF25 412AD000 9F3D5EB7
                                                                                         .Lj{.%j.+J. :Zj..9...8W...%A*. .=^.
                                                                                        ...W"j" ...W .-..$..Hce.j..Vf.7 D..V
..^J<.. MEC.. ..Your flag is: "picoC
     8EA9C557 226A2206 B5A7CB57 16B32DDA AF2495BC 486365F9 6A9CAD56 66AA370D 44808A56
76068 A4A85E4A 3CCDD520 4D4543BA 8A00FFD9 596F7572 20666C61 67206973 3A202270 69636F43
                                                                                        TF{and_thats_how_u_edit_hex_kittos_8
76104 54467B61 6E645F74 68617473 5F686F77 5F755F65 6469745F 6865785F 6B697474 6F735F38
76140 42634136 3761327D 220A
                                                                                        BcA67a2}"
Signed Int 🗘 le, dec (select some data)
                                                                                                                           76084 out of 76150 bytes
```

可以看到到jpg文件格式的结尾FF D9之后还有一串字符,就是我们要的flag。

flag:picoCTF{and_thats_how_u_edit_hex_kittos_8BcA67a2}

Truly an Artist

Question

Can you help us find the flag in this <u>Meta-Material</u>? You can also find the file in /problems/truly-an-artist 3 066d6319e350c1d579e5cf32e326ba02.

Hint

Try looking beyond the image.

Who created this?

Solution

文件属性隐藏了信息, windows下直接右键查看文件属性就可以看到, mac可以使用exiftool查看。

> exiftool 2018.png

ExifTool Version Number : 11.11
File Name : 2018.png
Directory : .
File Size : 13 kB

File Modification Date/Time : 2018:10:28 01:06:38+08:00 File Access Date/Time : 2018:10:28 01:06:50+08:00

File Inode Change Date/Time : 2018:10:28 01:06:51+08:00

: rw-r--r--File Permissions File Type Extension
MIME Type
Image Width : PNG : png : image/png : 1200 : 630 Image Height . 8
: RGB
: Deflate/)
: Adaptive
: Noninterl
: picoCTF{1 : 8 Bit Depth Color Type

: Deflate/Inflate Compression

Filter : Noninterlaced Interlace

: picoCTF{look_in_image_7e31505f} Artist

: 1200x630 Image Size : 0.756 Megapixels

flag:picoCTF{look_in_image_7e31505f}

now you don't

Question

We heard that there is something hidden in this <u>picture</u>. Can you find it?

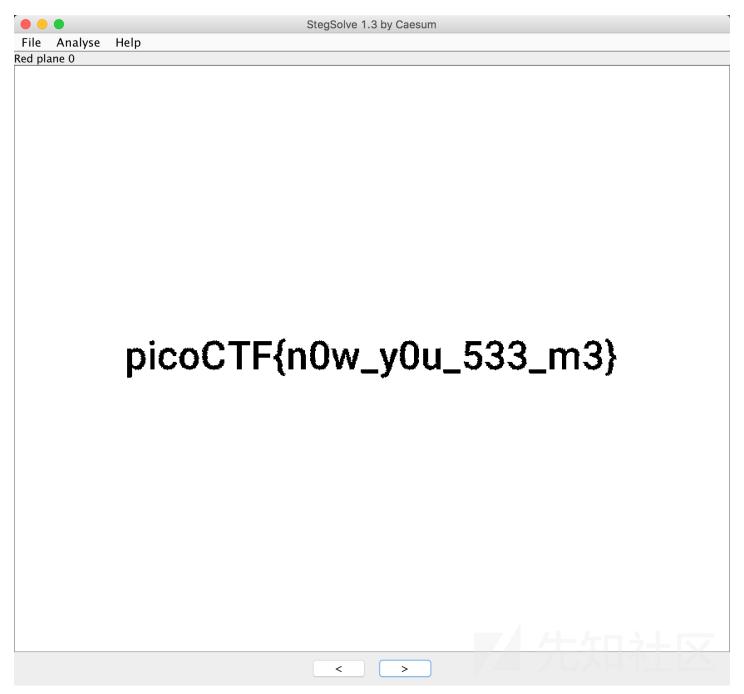
Hint

There is an old saying: if you want to hide the treasure, put it in plain sight. Then no one will see it.

Is it really all one shade of red?

Solution

还是用stegsolve打开文件,查看不同信道下的图片,发现flag在隐藏在红色0信道中。



flag:picoCTF{n0w_y0u533_m3}

Ext Super Magic

Question

We salvaged a ruined Ext SuperMagic II-class mech recently and pulled the <u>filesystem</u> out of the black box. It looks a bit corrupted, but maybe there's something interesting in there. You can also find it in /problems/ext-super-magic_4_f196e59a80c3fdac37cc2f331692ef13 on the shell server.

Hint

Are there any tools for diagnosing corrupted filesystems? What do they say if you run them on this one?

How does a linux machine know what type of file a file is?

You might find this doc helpful.

Be careful with endianness when making edits.

Once you've fixed the corruption, you can use \slash sbin/ \slash to pull the flag file out.

Solution

```
给了一个镜像文件,file命令查看一下,发现不能识别。debugfs可以识别出镜像损坏的部分。
```

```
> file ext-super-magic.img
ext-super-magic.img: data
> debugfs ext-super-magic.img
debugfs 1.44.1 (24-Mar-2018)
Checksum errors in superblock! Retrying...
ext-super-magic.img: Bad magic number in super-block while opening filesystem
```

依据提示查看ext2镜像格式的文档,我们需要在superblock的第56和57字节之间插入magic number,即0xef53。

```
> file fixed.img
```

fixed.img: Linux rev 1.0 ext2 filesystem data, UUID=fad5d44e-2bb4-4c22-9410-79b020de84dd (large files)

修复成功,挂载打开,发现有很多的jpg文件,其中有一张flag.jpg里面就有flag。

Your flag is: "picoCTF (a7DB29eCf7dB9960f0A19Fdde9d00Af0)"

flag:picoCTF{a7DB29eCf7dB9960f0A19Fdde9d00Af0}

Lying Out

Question

Some odd traffic has been detected on the network, can you identify it? More info here. Connect with no 2018shell1.picoctf.com 50875 to help us answer some questions.

Hint

No Hints.

Solution

需要分析异常访问流量,对照图片一个个看就可以了。

You'll need to consult the file `traffic.png` to answer the following questions.

Which of these logs have significantly higher traffic than is usual for their time of day? You can see usual traffic on the at

```
time num_IPs
  log_ID
      0 00:00:00
                    9552
      1 02:30:00 11573
1
       2 06:00:00 10381
2
      3 07:00:00 11674
3
                  10224
       4 07:00:00
4
      5 07:30:00
                  10966
5
      6 16:00:00
6
                    9685
                  15875
      7 17:45:00
7
      8 18:00:00 11889
8
                  11935
      9 19:15:00
9
10
      10 19:30:00
                  11191
      11 20:30:00
                    9952
11
      12 20:45:00
                    9898
12
      13 22:45:00 11609
13
1 3 7 13
Correct!
Great job. You've earned the flag: picoCTF\{w4y_0ut_ff5bd19c\}
```

flag:picoCTF{w4y_Out_ff5bd19c}

What's My Name?

Question

Say my name, say my name.

Hint

If you visited a website at an IP address, how does it know the name of the domain?

Solution

提示给的很明显了,我们需要查找和DNS有关的信息流,在wireshark过滤器中搜寻dns流量,就可以看到flag了。

dns					
10.	Time	Source	Destination	Protocol	Lengt
-	43 1418.341495	192.168.2.1	192.168.2.12	DNS	8
_	55 1418.342859	192.168.2.12	192.168.2.1	DNS	31

Time to live: 300 Data length: 55 TXT Length: 54

TXT: picoCTF{w4lt3r_wh1t3_33ddc9bcc77f22a319515c59736f64a2} c0 a8 02 0d c0 0c 00 05 0050 00 01 00 00 01 2c 00 04 0060 00 01 00 00 01 2c 00 09 06 6d 79 6e 61 6d 65 c0 ·myname · 0070 19 c0 0c 00 0f 00 01 00 00 01 2c 00 04 00 05 c0 00 01 2c 00 08 00 0a 03 0080 3e c0 0c 00 0f 00 01 00 0090 6d 78 32 c0 3e c0 0c 00 0f 00 01 00 00 01 2c 00 mx2·>··· 00a0 08 00 14 03 6d 78 33 c0 3e c0 0c 00 02 00 01 00 · · · · mx3 · > · · 00b0 01 51 80 00 06 03 6e 73 31 c0 3e c0 0c 00 02 00 ·0···ns 1·>··· 6e 73 32 00c0 01 00 01 51 80 00 06 03 c0 3e c0 · · · 0 · · · · ns2 · > · · · 0c 00 6f 43 54 00d0 10 00 01 00 00 01 2c 00 37 36 70 69 63 ·····, · 76picoCT 00e0 46 7b 77 34 6c 74 33 72 5f 77 68 31 74 33 5f 33 F{w4lt3r wh1|t|3 3 00f0 33 64 64 63 39 62 63 63 37 37 66 32 32 61 33 31 3ddc9bcc 77f22a31 35 31 35 63 35 39 37 33 36 66 36 34 61 32 9515c597 36f64a2} 0100 39 CO OC OO OF OO O1 OO O1 51 80 00 20 03 66 73 31

同样也可以通过字符串搜索的方式找到flag,方法和admin panel一样。

Malware Shopscore

There has been some malware detected, can you help with the analysis? More info here. Connect with no 2018shell1.picoctf.com 18874.

Hint

No Hints.

Solution

还是看图识别数据,和Lying

Out差不大多,第一个问题看图片找特征,第二个问题看哪个文件与题目问的文件的jmp_count和add_count的数值相近就选哪个。

You'll need to consult the file `clusters.png` to answer the following questions.

How many attackers created the malware in this dataset?

Correct!

In the following sample of files from the larger dataset, which file was made by the same attacker who made the file 628e79cf?

hash jmp_count add_count

0	628e79cf	17.0	18.0
1	1f2c7915	18.0	60.0
2	6e7d554a	10.0	42.0
3	a55f572c	30.0	37.0
4	f118fcd7	36.0	13.0
5	97b1425e	35.0	30.0
6	a163e543	18.0	71.0
7	ebaf5ccd	11.0	18.0
8	9059414f	38.0	13.0
9	c30ea3fe	18.0	37.0

ebaf5ccd

Correct!

Great job. You've earned the flag: picoCTF{w4y_Out_deal794b}

点击收藏 | 0 关注 | 1

上一篇: Cutwail垃圾邮件活动用隐写术... 下一篇: Symmetric block c...

- 1. 0 条回复
 - 动动手指,沙发就是你的了!

登录后跟帖

先知社区

现在登录

热门节点

技术文章

<u>社区小黑板</u>

目录

RSS 关于社区 友情链接 社区小黑板