

Write-Up jumat-sabtu 29-30/04/2022

Forensic

CTF

1. extensions (<https://play.picoctf.org/practice/challenge/52?category=4&page=2>)

- Diberikan sebuah file txt. Saat di lihat ternyata format filenya berupa file png

```
(root@utab) - [/home/utab/Desktop]  
# cat flag\_(1\).txt  
PNG
```

- Langsung saja dibuat copy-an dari file tersebut dengan .png file

```
(root@utab) - [/home/utab/Desktop]  
# cp flag\_(1\).txt flag.png
```

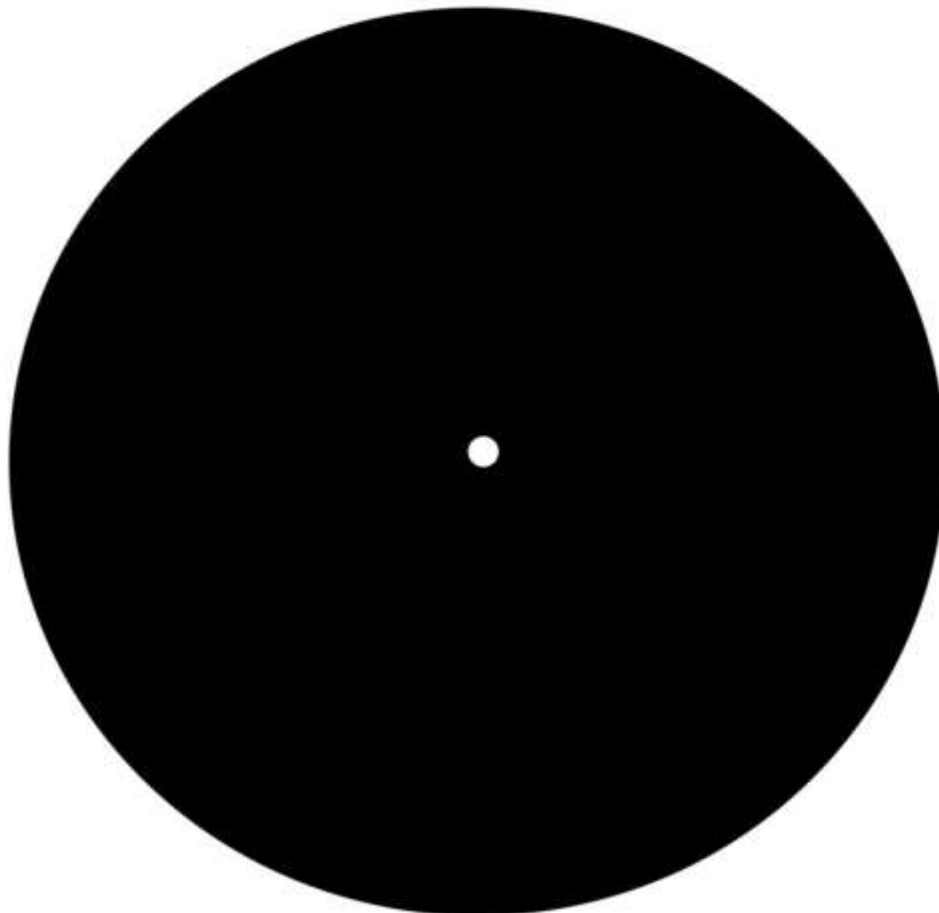
- Setelah dibuka ternyata berisi gambar flagnya

picoCTF{now_you_know_about_extensions}

picoCTF{now_you_know_about_extensions}

2. Enhance! (<https://play.picoctf.org/practice/challenge/265?category=4&page=1>)

- Didapat sebuah file gambar dalam bentuk html



- Setelah di inspect, ternyata flagnya ada di baris codingannya

```
>p </tspan><tspan
"line"

ze:0.00352781px;line-height:
>i </tspan><tspan
"line"

ze:0.00352781px;line-height:
>c </tspan><tspan
"line"

ze:0.00352781px;line-height:
>o </tspan><tspan
"line"

ze:0.00352781px;line-height:
>C </tspan><tspan
"line"

ze:0.00352781px;line-height:
>T </tspan><tspan
"line"

ze:0.00352781px;line-height:
>F { 3 n h 4 n </tspan><tspan
"line"

ze:0.00352781px;line-height:
>c 3 d _ d 0 a 7 5 7 b f }</
```

picoCTF{3nh4nc3d_d0a757bf}

- Looky here (<https://play.picoctf.org/practice/challenge/279?category=4&page=1>)



- Lalu saat di tampilan, berisi informasi yang sangat banyak



- Lalu saat di grep, flagnya pun didapat

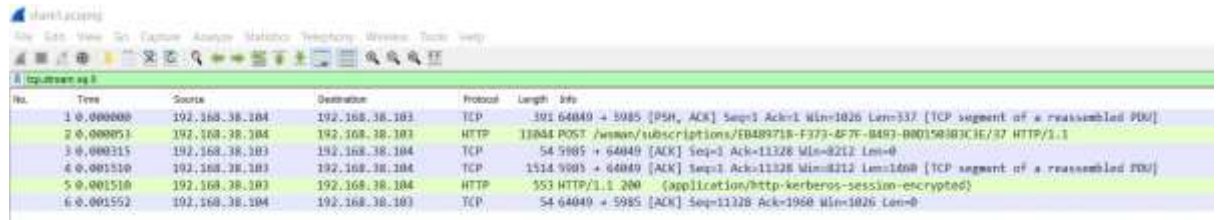
```
(root@utab) - [ /home/utab/Desktop ]
# cat anthem.flag.txt | grep picoCTF
we think that the men of picoCTF{gr3p_15_@w3s0m3_2116b979}

picoCTF{gr3p_15_@w3s0m3_2116b979}
```

4. Wireshark doo dooo do doo...

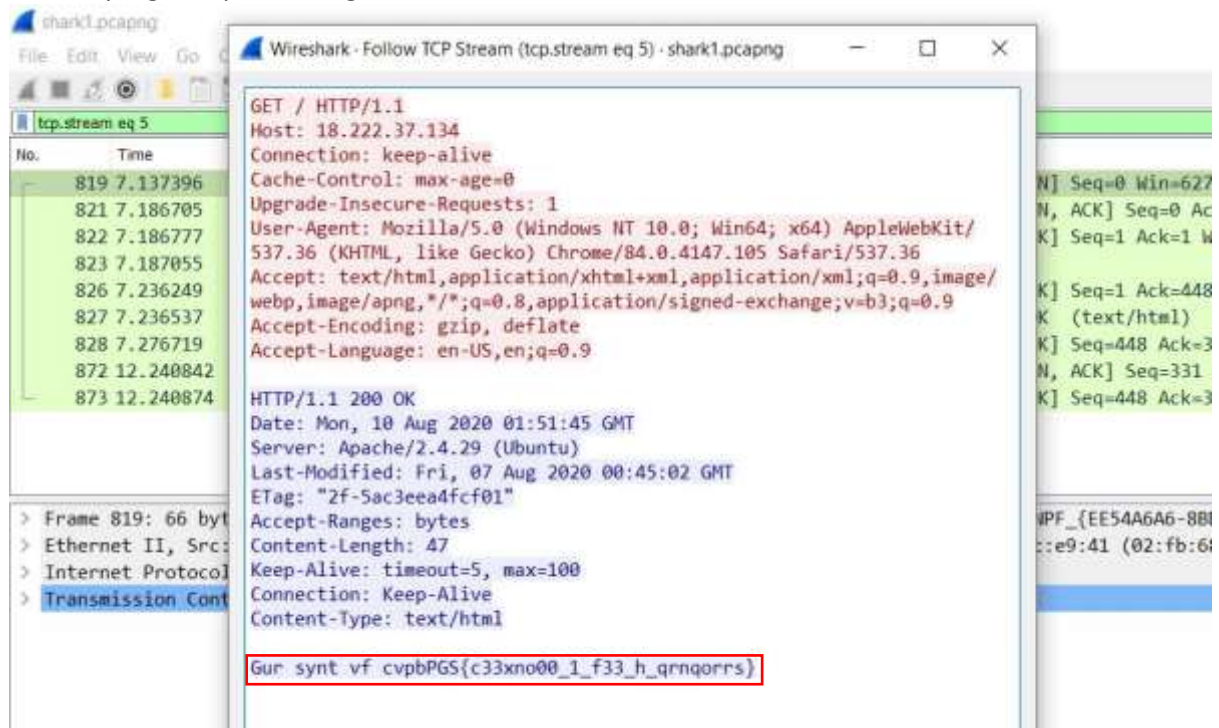
(<https://play.picoctf.org/practice/challenge/115?category=4&page=1>)

- Diberikan sebuah file wireshark



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|---|
| 1 | 0.000000 | 192.168.38.104 | 192.168.38.103 | TCP | 302 | 64040 → 5085 [PSH, ACK] Seq=1 Ack=1 Win=1026 Len=337 [TCP segment of a reassembled PDU] |
| 2 | 0.000051 | 192.168.38.104 | 192.168.38.103 | HTTP | 11044 | POST /woman/subscriptions/EB489718-F373-4F7E-B493-B001548B3CE/37 HTTP/1.1 |
| 3 | 0.000315 | 192.168.38.103 | 192.168.38.104 | TCP | 54 | 5085 → 64040 [ACK] Seq=1 Ack=11328 Win=8212 Len=0 |
| 4 | 0.001510 | 192.168.38.103 | 192.168.38.104 | TCP | 1514 | 5085 → 64040 [ACK] Seq=1 Ack=11328 Win=8212 Len=1400 [TCP segment of a reassembled PDU] |
| 5 | 0.001510 | 192.168.38.103 | 192.168.38.104 | HTTP | 553 | HTTP/1.1 200 (application/http-kberos-session-encrypted) |
| 6 | 0.001552 | 192.168.38.104 | 192.168.38.103 | TCP | 54 | 64040 → 5085 [ACK] Seq=11328 Ack=1960 Win=1026 Len=0 |

- Setelah mengganti “tcp.stream eq” menjadi “5” lalu dilihat TCP streamnya ditemukan kalimat yang cukup mencurigakan



Wireshark - Follow TCP Stream (tcp.stream eq 5) - shark1.pcapng

```
GET / HTTP/1.1
Host: 18.222.37.134
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Date: Mon, 10 Aug 2020 01:51:45 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Fri, 07 Aug 2020 00:45:02 GMT
ETag: "2f-5ac3eea4fcf01"
Accept-Ranges: bytes
Content-Length: 47
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Gur synt vf cvpbPGS{c33xno00_1_f33_h_qrnqorrs}
```

- Setelah itu dicobalah di decrypt kalimat tersebut dengan ROT13 dan dapatlah flagnya

The flag is
picoCTF{p33kab00_1_s33_u_deadbeef}
picoCTF{p33kab00_1_s33_u_deadbeef}

Tool

Crunch

[https://docs.google.com/spreadsheets/d/12-](https://docs.google.com/spreadsheets/d/12-PmcG_1MtY2hXDoBvjCHuLQEUTXaw/edit#gid=1427959827&range=E12)

[PmcG_1MtY2hXDoBvjCHuLQEUTXaw/edit#gid=1427959827&range=E12](https://docs.google.com/spreadsheets/d/12-PmcG_1MtY2hXDoBvjCHuLQEUTXaw/edit#gid=1427959827&range=E12)

[https://docs.google.com/spreadsheets/d/12-](https://docs.google.com/spreadsheets/d/12-PmcG_1MtY2hXDoBvjCHuLQEUTXaw/edit#gid=1427959827&range=E13)

[PmcG_1MtY2hXDoBvjCHuLQEUTXaw/edit#gid=1427959827&range=E13](https://docs.google.com/spreadsheets/d/12-PmcG_1MtY2hXDoBvjCHuLQEUTXaw/edit#gid=1427959827&range=E13)

Tool ini digunakan untuk membuat wordlist yang dapat digunakan untuk melakukan bruteforce pada sebuah file yang memiliki keamanan seperti file zip yang diberi password

Ini merupakan hasil dari perintah untuk membuat random generated character

```
(root@utab) - [ /home/utab/Desktop ]
# crunch 4 4 -t @,%^
Crunch will now generate the following amount of data: 1115400 bytes
1 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 223080
aA0!
aA0@
aA0#
aA0$
aA0%
aA0^
aA0&
aA0*
aA0(
aA0)
aA0-
aA0_
aA0+
aA0=
aA0~
aA0`
aA0[
```

- @ = lowercase
- , = uppercase
- % = angka
- ^ = special character
- 4 | = banyak character awal
- | 4 = banyak character akhir

Agar hasilnya dapat disimpan pada sebuah file maka ditambahkan "-o [namafile]"

```
(root@utab) - [ /home/utab/Desktop ]
# crunch 4 4 -t 1,%^ -o bruteforce.txt
Crunch will now generate the following amount of data: 42900 bytes

~/Desktop/bruteforce.txt [Read Only] - Mousepad
File Edit Search View Document Help
1 1A0!
2 1A0@
3 1A0#
4 1A0$
5 1A0%
6 1A0^
7 1A0&
8 1A0*
```