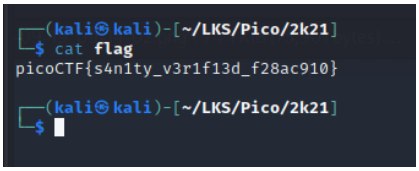
PicoCTF 2021
Ahmad Ryan Faizal

Obedient Cat

This file has a flag in plain sight (aka "in-the-clear"). Download flag.

Sesuai soal flag ada di plain sight berarti mudah saja langsung cat dan ya benar saja flagnya langsung keliatan

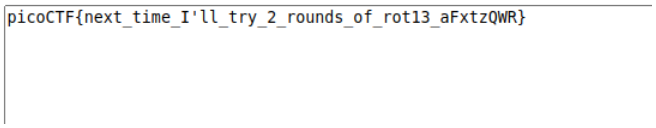


picoCTF{next_time_I'll_try_2_rounds_of_rot13_aFxtzQWR}

Mod26

Cryptography can be easy, do you know what ROT13 is?
cvpbPGS{arkg_gvzr_V'yy_gel_2_ebhaqf_bs_ebg13_nSkgmDJE}

Sesuai soal ditanyakan rot13 maka langsung saja saya convert dengan web rot13



picoCTF{next_time_I'll_try_2_rounds_of_rot13_aFxtzQWR}

Python Wrangling

Python scripts are invoked kind of like programs in the Terminal... Can you run this Python script using this password to get the flag?

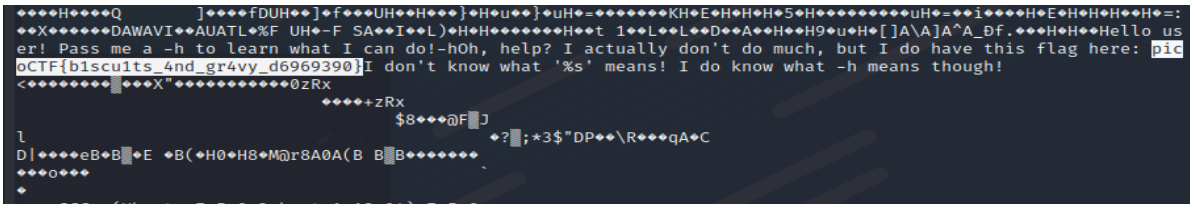
Sesuai soal disuruh menjalankan program yang sudah disediakan lalu mendapatkan flag dengan menggunakan password yang disediakan juga

Pertama-tama saya liat apa password tersebut setalah mendapatkannya saya langsung menjalankan programnya ternyata memiliki dua opsi antara -e/-d lalu dimasukkan file yang ingin didapatkan yang disini kondisinya flag. Saya coba saja dua-duanya dan ya benar flagnya didapatkan

Wave a flag

Can you invoke help flags for a tool or binary? This program has extraordinarily helpful Disediakan program ‘warm’ karena sudah kebiasaan saya sebelum menjalankan suatu *information...*

file/program selalu saya ‘cat’ ataupun ‘nano’ file tersebut dan setelah saya cat saya lihat flagnya langsung muncul.



picoCTF{b1scu1ts_4nd_gr4vy_d6969390}

Alternative / Actual Way

Karena file tidak bisa dieksekusi dengan alasan “permission denied” maka saya ubah dengan permissionnya dengan menggunakan “chmod”

```
┌──(kali㉿kali)-[~/LKS/Pico/2k21/Wave_a_flag]
└─$ chmod +x warm

┌──(kali㉿kali)-[~/LKS/Pico/2k21/Wave_a_flag]
└─$ ./warm
Hello user! Pass me a -h to learn what I can do!

┌──(kali㉿kali)-[~/LKS/Pico/2k21/Wave_a_flag]
└─$ ./warm -h
Oh, help? I actually don't do much, but I do have this flag here: picoCTF{b1scu1ts_4nd_gr4vy_d6969390}
```

picoCTF{b1scu1ts_4nd_gr4vy_d6969390}

information

Files can always be changed in a secret way. Can you find the flag? cat.jpg

Diberikan hint “look at the details of the file” tanpa basa-basi karena sebelumnya saya juga sudah biasa melihat details dari file langsung saja saya lihat menggunakan exiftool dan disana ada beberapa karakter yang mencurigakan yaitu “7a78f3d9cfb1ce42ab5a3aa30573d617” dan “cGljb0NURnt0aGVfbTN0YWRhdGFfMXNfbW9kaWZpZWR9”

```
└─$ exif cat.jpg
Corrupt data
The data provided does not follow the specification.
ExifLoader: The data supplied does not seem to contain EXIF data.

┌──(kali㉿kali)-[~/LKS/Pico/2k21/information]
└─$ exiftool cat.jpg
ExifTool Version Number         : 12.44
File Name                       : cat.jpg
Directory                       : .
File Size                       : 878 kB
File Modification Date/Time     : 2021:03:15 14:24:46-04:00
File Access Date/Time           : 2022:09:19 09:46:04-04:00
File Inode Change Date/Time     : 2022:09:19 09:45:58-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.02
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Current IPTC Digest             : 7a78f3d9cfb1ce42ab5a3aa30573d617
Copyright Notice                : PicoCTF
Application Record Version      : 4
XMP Toolkit                     : Image::ExifTool 10.80
License                         : cGljb0NURnt0aGVfbTN0YWRhdGFfMXNfbW9kaWZpZWR9
Rights                          : PicoCTF
Image Width                     : 2560
Image Height                    : 1598
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
```

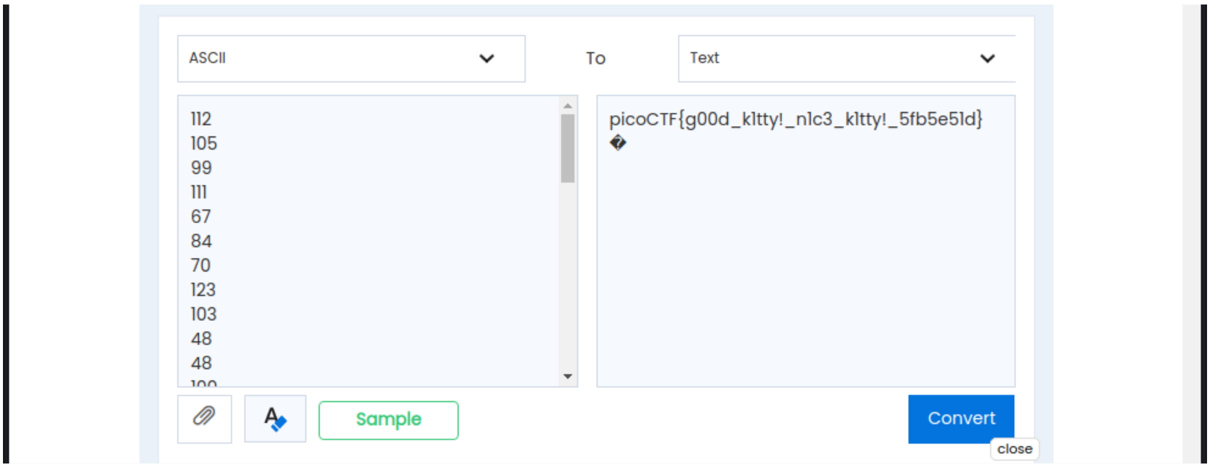
langsung coba saya decode di CyberChef dan CyberChef bisa mendeteksi bahwa salah satunya diencode menggunakan Base64 langsung saja saya decode dan keluarlah flagnya:

picoCTF{the_m3tadata_1s_modified}

Nice netcat..

There is a nice program that you can talk to by using this command in a shell: `$ nc mercury.picoctf.net 22342`*, but it doesn't speak English…*

Langsung saja saya coba netcat ke link yang sudah diberikan dan yang muncul adalah beberapa angka saya mengasumsikan itu adalah ASCII dan untuk memastikan kembali saya membuka hint yang diberikan dan yak benar saja ada hint yang berhubungan dengan ASCII maka saya convert menggunakan website ini



picoCTF{g00d_k1tty!_n1c3_k1tty!_5fb5e51d}

Information

I wonder what this really is... *enc* `''.join([chr((ord(flag[i]) << 8) + ord(flag[i + 1])) for i in range(0, len(flag), 2)])`

Disini saya sangatlah bingung dan tidak mempunyai clue apa yang harus dilakukan lalu saya coba membuka file flag yang terenkripsi tersebut dan muncullah “灩捯䍔䙻ㄶ形楴獟楮獴㌴摟潦弸弲㘶㠴挲ぽ”

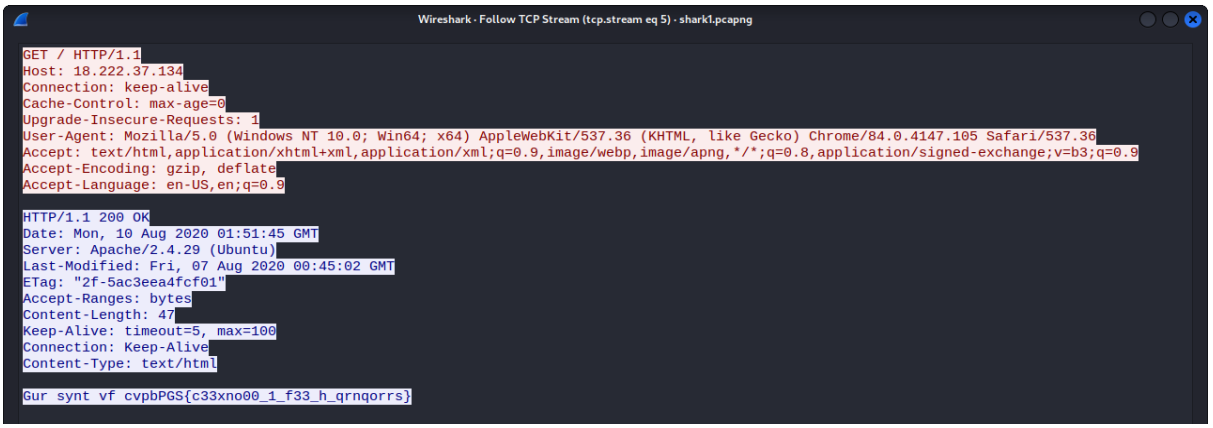
Disini saya berasumsi ini adalah flag yang terenkripsi dengan suatu bahasa karena saya bingung itu bahasa apa saya kembali menggunakan cyberchef dengan fitur ‘magic’-nya yang bisa detect dan decode berbagai bahasa dan ya setelah di dekripsi dengan berbagai bahasa langsung saja saya search pico dan ketemu flagnya

picoCTF{16_bits_inst34d_of_8_e141a0f7}

Wireshark doo dooo do doo…

Can you find the flag? shark1.pcapng.

Setelah membuka filenya langsung saja saya follow TCP Stream sampai pada stream ke 5 saya menemukan suatu teks yang berbentuk seperti format ctf



Gur synt vf cvpbPGS{c33xno00_1_f33_h_qrnqorrs}

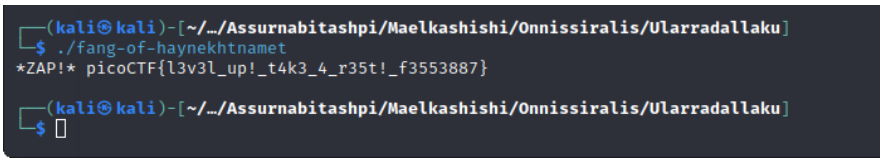
karena saya lumayan familiar dengan rot13 maka saya langsung tau ini rot13 dari “vf” karena vf jika di decrypt menggunakan rot13 adalah is. Maka langsung saja saya menggunakan web rot13 seperti biasa dan muncullah flag

The flag is picoCTF{p33kab00_1_s33_u_deadbeef}

Tab, Tab, Attack

Using tabcomplete in the Terminal will add years to your life, esp. when dealing with long rambling directory structures and filenames: Addadshashanammu.zip

Saya mulai dengan mengunzip file tersebut didalam file tersebut ada beberapa lipat direktori jadi saya melihat sampai direktori terakhri dan ada file yang jika dijalankan akan memberikan flag

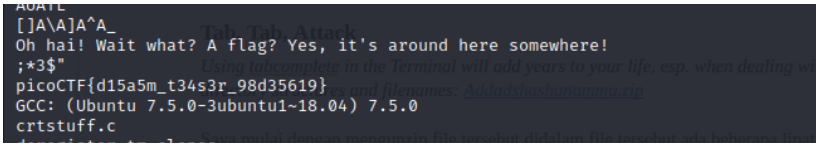


picoCTF{l3v3l_up!_t4k3_4_r35t!_f3553887}

Static ain't always noise

Can you look at the data in this binary: static? This BASH script might help!

Diberikan file static (?) dan juga script. Alih-alih menjalankan script yang diberikan saya melakukan strings pada file ‘static’ untuk melihat beberapa printable character dan ternyata ada flag didalamnya

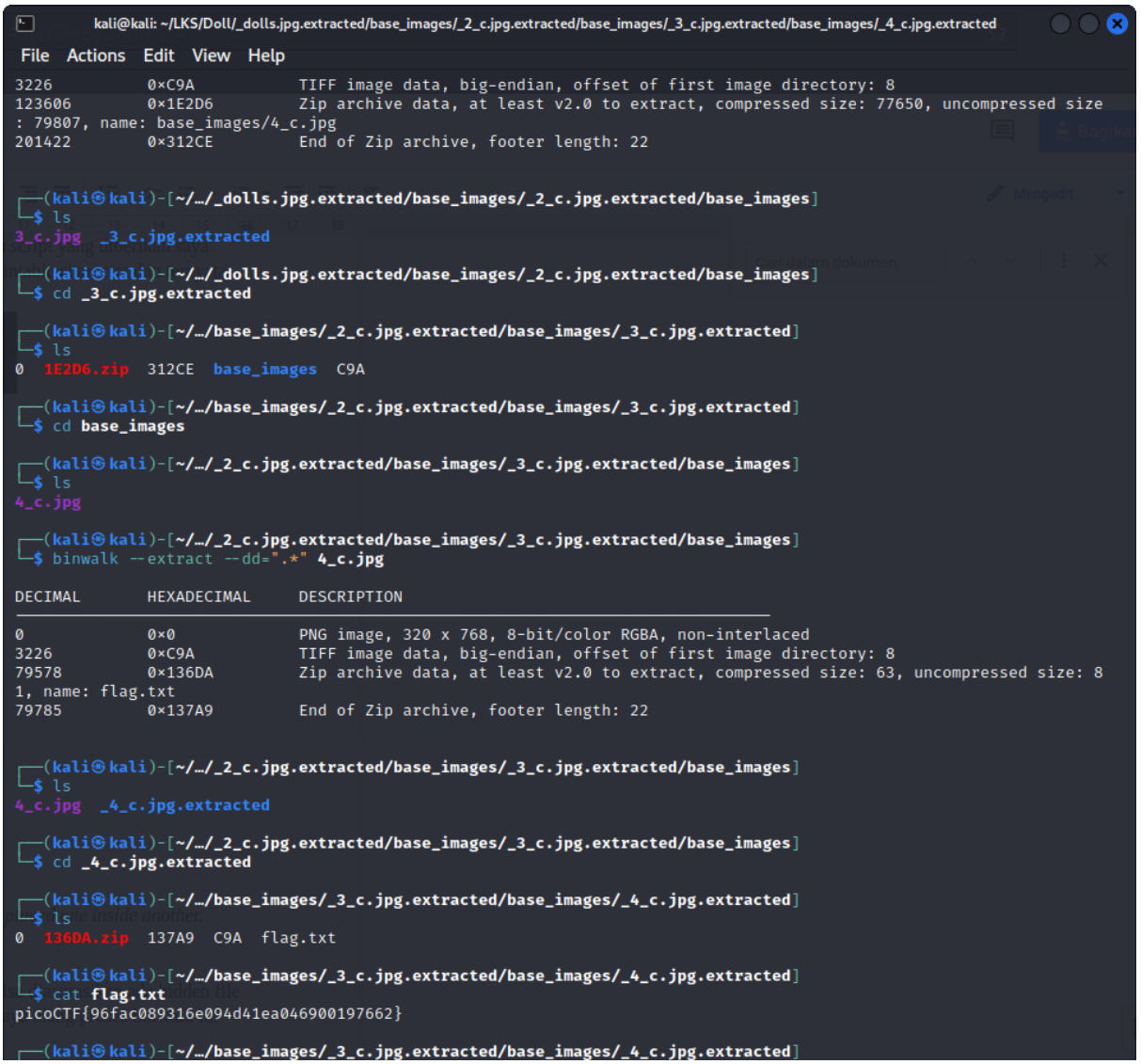


picoCTF{d15a5m_t34s3r_98d35619}

Matryoshka doll

Matryoshka dolls are a set of wooden dolls of decreasing size placed one inside another. What's the final one? Image: this

Diadakan file image dan ada soal “one inside another” yang bisa diasumsikan ada hidden file dan benar saja ketika di binwalk ada hidden file yang keluar saya ulang proses binwalk ini sampai akhir dan pada akhirnya ketemu flag.txt

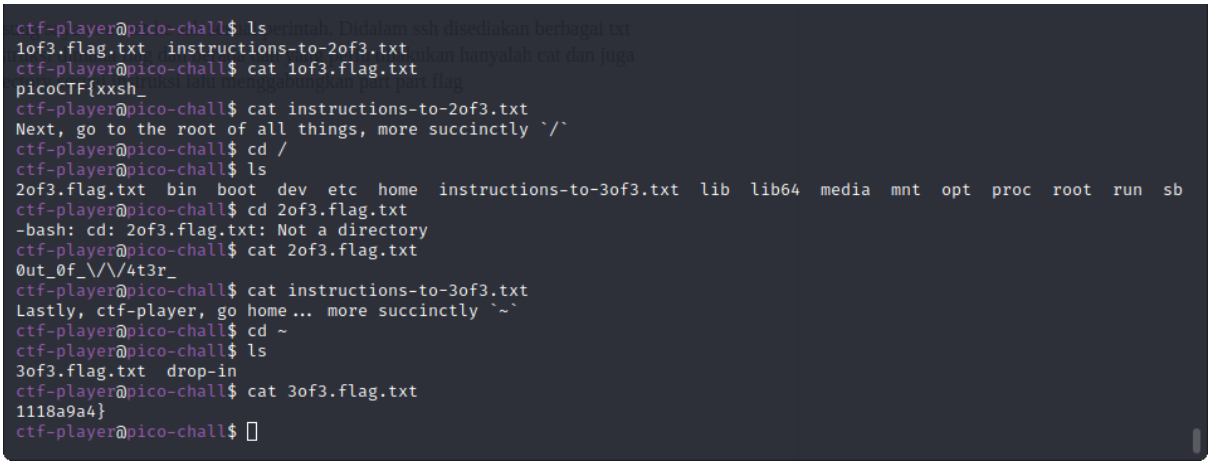


picoCTF{96fac089316e094d41ea046900197662}

Magikarp Ground Mission

Do you know how to move between directories and read files in the shell? Start the container, `ssh` to it, and then `ls` once connected to begin. Login via `ssh` as `ctf-player` with the password, `481e7b14`

disini langsung saya connect ke ssh sesuai perintah. Didalam ssh disediakan berbagai txt sebagai instruksi dimana flag dan berada dan yang perlu dilakukan hanyalah cat dan juga change directory sesuai instruksi lalu menggabungkan part part flag



didapatkan lah:
picoCTF{xxsh_0ut_0f_\/\/4t3r_1118a9a4}