

Obedient Cat

5 points

Tags:

Category: General Skills

AUTHOR: SYREAL

Description

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

Hints

123

63,848 solves / 99,012 attempts (64%)

89% Liked

🚩 picoCTF{FLAG}

Submit Flag

```
(biddion@kali)-[~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
$ cat flag
picoCTF{s4n1ty_v3r1f13d_b5aeb3dd}
```

It's a simple as downloading the file and cat'ing it.

Python Wrangling

10 points

Tags:

Category: General Skills

AUTHOR: SYREAL

Description

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

Hints

12

\$ man python

32,822 solves / 46,753 attempts (70%)

62% Liked

🚩 picoCTF{FLAG}

Submit Flag

This is the syntax I've been needing to do the mini competition challenges

```
python3 ende.py -d flag.txt.en $(cat pw.txt)
```

-d is to turn on parser debugging output; i don't know what the means YET
man python has nothing about \$ but I'm going to assume its a variable.

```
(biddion@kali)-[~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
$ ls
ende.py  flag  flag.txt.en  pw.txt

(biddion@kali)-[~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
$ python3 ende.py -d flag.txt.en $(cat pw.txt)
picoCTF{4p0110_1n_7h3_h0us3_aa821c16}
```

Wave a flag

10 points

Tags:

Category: General Skills

AUTHOR: SYREAL

Description

Can you invoke help flags for a tool or binary? [This program](#) has extraordinarily helpful information...

39,310 solves / 48,921 attempts (80%)

Hints

1

2

3

4

5

To get the file accessible in your shell, enter the following in the Terminal prompt: `$ wget https://mercury.picoctf.net/static/a14be2648c73e3cda5fc8490a2f476af/warm`

90% Liked

```
(biddion@kali) [~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
$ file warm
warm: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x84.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=3181a501366281ab5eba1c41e54a1f40800e3966, with debug_info, not stripped

(biddion@kali) [~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
$ chmod 777 warm

(biddion@kali) [~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
$ ./warm
Hello user! Pass me a -h to learn what I can do!

(biddion@kali) [~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
$ ./warm -h
Oh, help? I actually don't do much, but I do have this flag here: picoCTF{b1scuits_4nd_gr4vy_755f3544}

(biddion@kali) [~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
$
```

downloaded warm; saw it was elf; changed permissions and ran it.

Nice netcat...

| 15 points

Tags: Category: General Skills

AUTHOR: SYREAL

Description

There is a nice program that you can talk to by using this command in a shell: `$ nc mercury.picoctf.net 43239`, but it doesn't speak English...

32,129 solves / 51,715 attempts (62%)

Hints

1

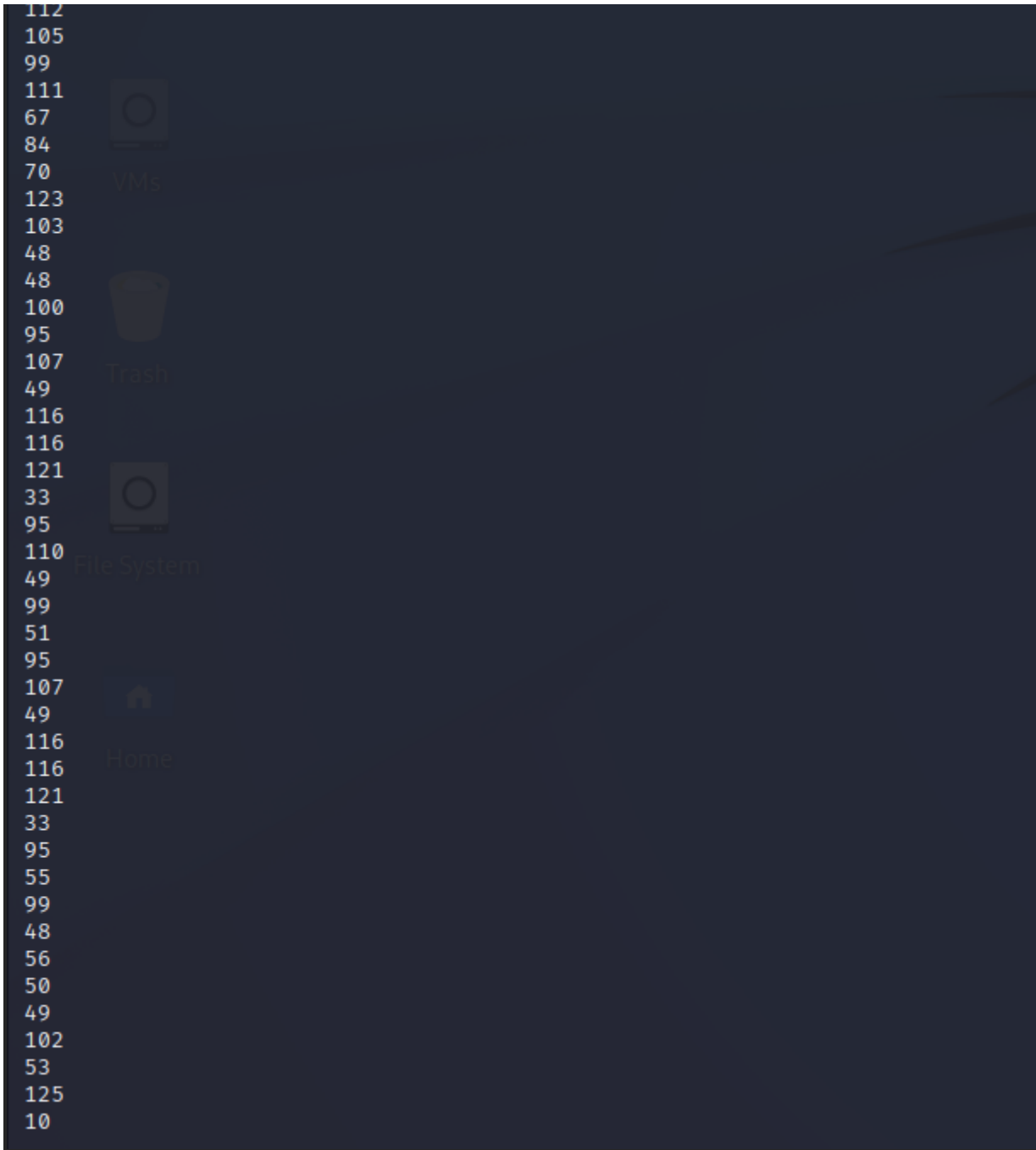
2

90% Liked

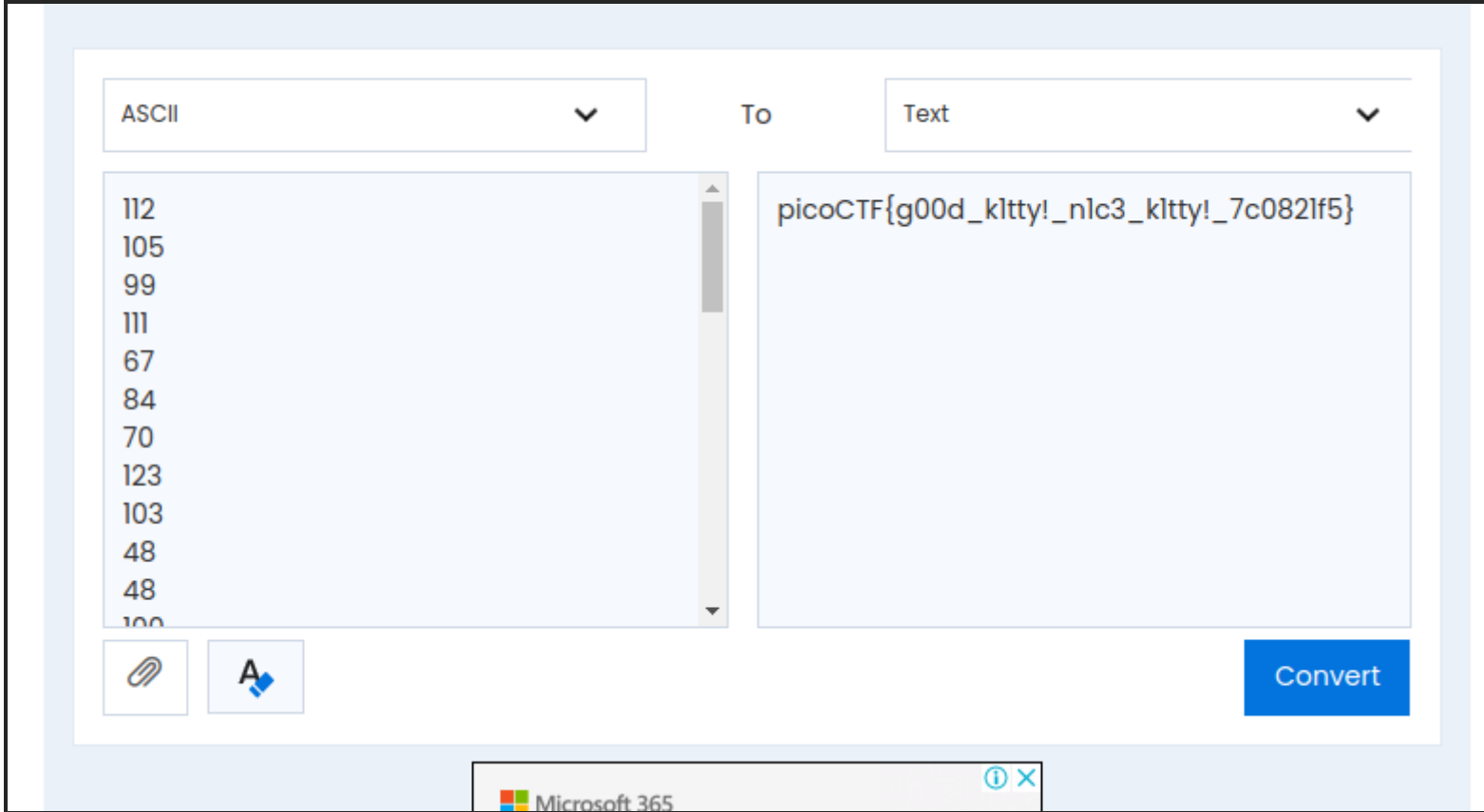
picoCTF{FLAG}

Submit Flag

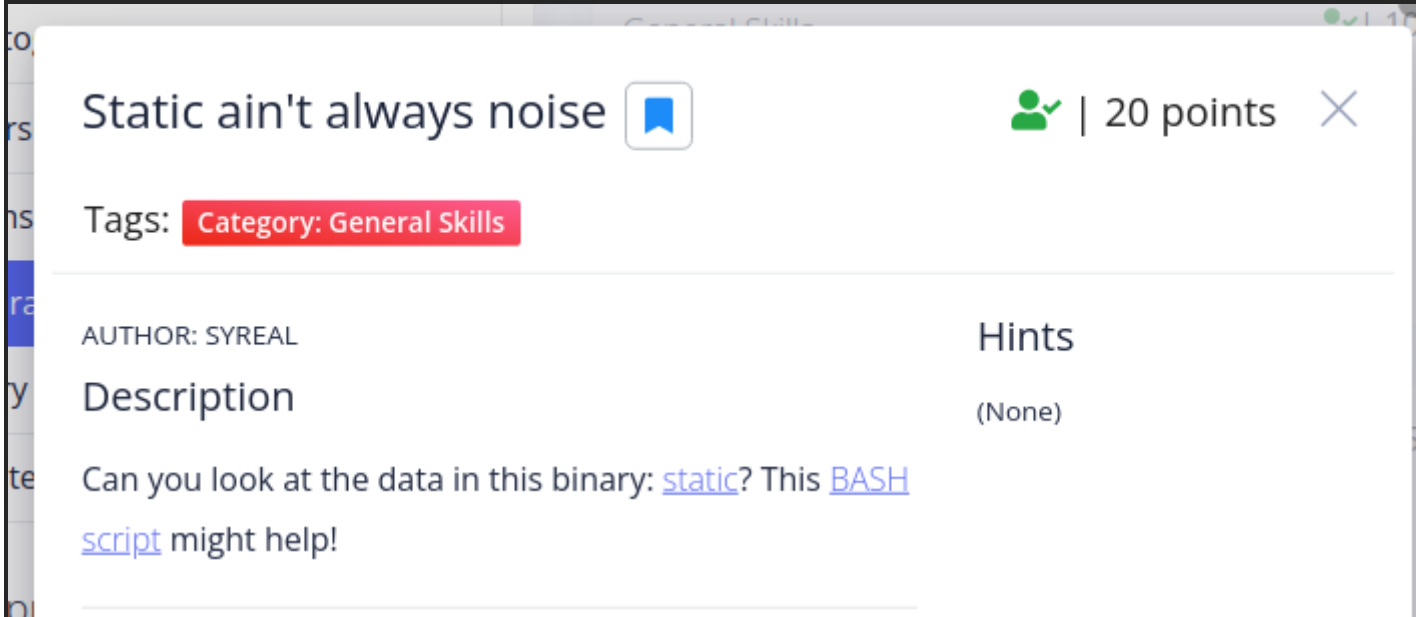
```
(biddion@kali) [~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
$ nc mercury.picoctf.net 43239
```



<https://www.duplichecker.com/ascii-to-text.php>



using net cat produces the ascii code; converting the code gives flag



19,169 solves / 21,941 attempts (87%)

86%

Liked

picoCTF{FLAG}

Submit

Flag

```
(biddion@kali)-[~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
$ ./ltdis.sh static
Attempting disassembly of static ...
Disassembly successful! Available at: static.ltdis.x86_64.txt
Ripping strings from binary with file offsets ...
Any strings found in static have been written to static.ltdis.strings.txt with file offset

(biddion@kali)-[~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
$
```

```
(biddion@kali)-[~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
$ cat static.ltdis.strings.txt | grep 'pico'
1020 picoCTF{d15a5m_t34s3r_1e6a7731}

(biddion@kali)-[~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
```

running binary with "static" as argument results in static.ltdis.string.text; grepping "pico" for the win

Tab, Tab, Attack

20 points

Tags:

Category: General Skills

AUTHOR: SYREAL

Description

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

[Addadshashanammu.zip](#)

Hints

1

19,455 solves / 24,901 attempts (78%)

82%

Liked

picoCTF{FLAG}

Submit

Flag

```
(biddion@kali)-[~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
$ unzip Addadshashanammu.zip
Archive:  Addadshashanammu.zip
  creating: Addadshashanammu/
  creating: Addadshashanammu/Almurbalarammi/
  creating: Addadshashanammu/Almurbalarammi/Ashalmimilkala/
  creating: Addadshashanammu/Almurbalarammi/Ashalmimilkala/Assurnabitashpi/
  creating: Addadshashanammu/Almurbalarammi/Ashalmimilkala/Assurnabitashpi/Maelkashishi/
  creating: Addadshashanammu/Almurbalarammi/Ashalmimilkala/Assurnabitashpi/Maelkashishi/Onnissiralis/
  creating: Addadshashanammu/Almurbalarammi/Ashalmimilkala/Assurnabitashpi/Maelkashishi/Onnissiralis/Ularradallaku/
  inflating: Addadshashanammu/Almurbalarammi/Ashalmimilkala/Assurnabitashpi/Maelkashishi/Onnissiralis/Ularradallaku/fang-of-haynekhtnamet

(biddion@kali)-[~/Documents/GitHub/picoCTF/Gym_GeneralSkills]
$ unzip Addadshashanammu/Almurbalarammi/Ashalmimilkala/Assurnabitashpi/Maelkashishi/Onnissiralis/Ularradallaku/fang-of-haynekhtnamet [Addadshashanammu/Almurbalarammi/Ashalmimilkala/Assurnabitashpi/Maelkashishi/Onnissiralis/Ularradallaku/fang-of-haynekhtnamet]
```



```
attaku/fang-of-haynekhthnamet]
End-of-central-directory signature not found. Either this file is not
a zipfile, or it constitutes one disk of a multi-part archive. In the
8#TT 1tt$D♦♦♦♦Ne central directory and zipfile comment will be found on
♦♦ ♦♦0)@t disk(;;♦
mmu/Almurbalarammi/Ashalmimilkala/Assurnabitashpi/Maelkashishi/Onnissiralis/Ularradallaku/fang-o
(biddion@kali)-[~/.../Assurnabitashpi/Maelkashishi/Onnissiralis/Ularradallaku]
$ file fang-of-haynekhthnamet
fang-of-haynekhthnamet: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib
64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=e34ce4e4ee2f7ce7fb251c8f5ab036da9882bc55, not stripped

(biddion@kali)-[~/.../Assurnabitashpi/Maelkashishi/Onnissiralis/Ularradallaku]
$ chmod 777 *

(biddion@kali)-[~/.../Assurnabitashpi/Maelkashishi/Onnissiralis/Ularradallaku]
$ ./fang-of-haynekhthnamet
*ZAP!* picoCTF{l3v3l_up!_t4k3_4_r35t!_524e3dc4}

(biddion@kali)-[~/.../Assurnabitashpi/Maelkashishi/Onnissiralis/Ularradallaku]
$
```

apparently you can unzip levels in one command with tab key
run binary for win

Magikarp Ground Mission

30 points

Category: General Skills

AUTHOR: SYREAL

Description

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, `6d448c9c`

This challenge launches an instance on demand.

Its current status is:

NOT_RUNNING

Launch Instance

Hints

1

Finding a cheatsheet for bash would be really helpful!

15,383 solves / 26,561 attempts (58%)

88% Liked

picoCTF{FLAG}

Submit Flag

Magikarp Ground Mission

30 points

Category: General Skills

AUTHOR: SYREAL

Description

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, `6d448c9c`

This challenge launches an instance on demand.

Its current status is:

RUNNING

Instance Time Remaining:

59:36

Restart

CHALLENGE

ENDPOINTS

SSH

```
ssh ctf-player@venus.picoctf.net -p 57421
```

Instance

Hints

1

Finding a cheatsheet for bash would be really helpful!

```
(biddion@kali)-[~/Documents/GitHub/picoCTF]
$ ssh ctf-player@venus.picoctf.net -p 57421
The authenticity of host '[venus.picoctf.net]:57421 ([3.131.124.143]:57421)' can't be established.
ED25519 key fingerprint is SHA256:P1f6h95BrSVnJbm2AKhphfHHGEyAeThib/rN/AwKs24.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[venus.picoctf.net]:57421' (ED25519) to the list of known hosts.
ctf-player@venus.picoctf.net's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1041-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ctf-player@pico-chall$ ls
1of3.flag.txt  instructions-to-2of3.txt
ctf-player@pico-chall$ cat 1of3.flag.txt
picoCTF{xxsh_
ctf-player@pico-chall$
```

```
ctf-player@pico-chall$ cat instructions-to-2of3.txt
Next, go to the root of all things, more succinctly `~`
ctf-player@pico-chall$ cd /
ctf-player@pico-chall$ ls
2of3.flag.txt  boot  etc  instructions-to-3of3.txt  lib64  mnt  proc  run  srv  tmp  var
bin            dev  home  lib                        media  opt  root  sbin sys usr
ctf-player@pico-chall$ cat 2of3.flag.txt instructions-to-3of3.txt
0ut_of_\\/\4t3r_
Lastly, ctf-player, go home... more succinctly `~`
ctf-player@pico-chall$ cd ~
ctf-player@pico-chall$ ls
3of3.flag.txt  drop-in
ctf-player@pico-chall$ cat 3of3.flag.txt
5190b070}
```

ssh login > cat 1 of 3 > cd / > cat 2 of 3 / cd ~ cat 3 of 3 > celebrate

Lets Warm Up

50 points

Tags: Category: General Skills

AUTHOR: SANJAY C/DANNY TUNITIS

Description

If I told you a word started with 0x70 in hexadecimal, what would it start with in ASCII?

Hints

1

43,688 solves / 99,124 attempts (44%)

77% Liked

picoCTF{FLAG}

Submit Flag

Warmed Up

50 points

Tags:

Category: General Skills

AUTHOR: SANJAY C/DANNY TUNITIS

Description

What is 0x3D (base 16) in decimal (base 10)?

Hints

1

40,163 solves / 72,004 attempts (56%)

86% Liked

picoCTF{FLAG}

Submit Flag

Recipe

From Base

Radix

16

To Base

Radix

10

Input

0x3D

Output

61

2Warm

50 points

Cyberchef converted

Tags:

Category: General Skills

AUTHOR: SANJAY C/DANNY TUNITIS

Description

Can you convert the number 42 (base 10) to binary (base 2)?

Hints

1

42,217 solves / 96,185 attempts (44%)

81% Liked

picoCTF{FLAG}

Submit Flag

Last build: 5 months ago

Recipe

From Base

Radix

10

To Base

Radix

2

Input

length: 2
lines: 1

42

Output

start: 0 time: 0
end: 6 length: 6
length: 6 lines: 1

101010

picoCTF{101010}

what's a net cat?

| 100 points

Tags:

Category: General Skills

AUTHOR: SANJAY C/DANNY TUNITIS

Description

Using netcat (nc) is going to be pretty important. Can you connect to [jupiter.challenges.picoctf.org](#) at

Hints

1

port 64287 to get the flag?

30,672 solves / 40,474 attempts (76%)



85%

Liked



picoCTF{FLAG}

Submit
Flag

```
(biddion@kali)-[~/Documents/GitHub/picoCTF]
$ nc jupiter.challenges.picoctf.org 64287
You're on your way to becoming the net cat master
picoCTF{nEtCat_Mast3ry_284be8f7}
```

```
(biddion@kali)-[~/Documents/GitHub/picoCTF]
$
```

nc jupiter.challenges.picoctf.org 64287

strings it



| 100 points



Tags:

Category: General Skills

AUTHOR: SANJAY C/DANNY TUNITIS

Description

Hints

1