Static ain’t always noise

Description:

Can you look at the data in this binary: [static](https://mercury.picoctf.net/static/0f6ea599582dcce7b4f1ba94e3617baf/static)? This [BASH script](https://mercury.picoctf.net/static/0f6ea599582dcce7b4f1ba94e3617baf/ltdis.sh) might help!

To begin, we need to download some files using the wget command:

Wget https://mercury.picoctf.net/static/0f6ea599582dcce7b4f1ba94e3617baf/static

Wget https://mercury.picoctf.net/static/0f6ea599582dcce7b4f1ba94e3617baf/ltdis.sh

After that, we can run the shell command along with the static file:

Bash ltdis.sh static

When it’s finished, we are given a string and a x86 file. We can use the cat command to look into the string file and manually find the pico flag. So, we use:

cat static.ltdis.strings.txt

We are greeted with a wall of text, but there are strings that gives us hints when we are close to the flag. Here is a little snippet.

spingy-picoctf@webshell:~/GeneralSkills/static$ cat static.ltdis.strings.txt

238 /lib64/ld-linux-x86-64.so.2

361 libc.so.6

36b puts

370 \_\_cxa\_finalize

37f \_\_libc\_start\_main

391 GLIBC\_2.2.5

39d \_ITM\_deregisterTMCloneTable

3b9 \_\_gmon\_start\_\_

3c8 \_ITM\_registerTMCloneTable

660 AWAVI

667 AUATL

6ba []A\A]A^A\_

6e8 Oh hai! Wait what? A flag? Yes, it's around here somewhere!

7c7 ;\*3$"

1020 picoCTF{d15a5m\_t34s3r\_6f8c8200}

1040 GCC: (Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.0

1671 crtstuff.c